NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

January 30, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of CIP-006 and CIP-007. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred nine thousand dollars ($109,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201102978, WECC2012010727, WECC2012010728, WECC2012010729, and WECC2012010730 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 16, 2013, by and between WECC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-2263	WECC201102978	CIP-006-1	R1	Medium	$109,000
			WECC2012010727	CIP-006-3a	R5	Medium	
			WECC2012010728	CIP-007-1	R2	Medium	
			WECC2012010729	CIP-007-1	R3	Lower	
			WECC2012010730	CIP-007-1	R6	Medium	

CIP-006

The purpose statement of Reliability Standard CIP-006 provides: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1

CIP-006-1 R1 provides:

> R1. Physical Security Plan — The Responsible Entity[4] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).
> >
> > R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.
> >
> > R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.
> >
> > R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.
> >
> > R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

[4] Within the text of Standards CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.
>
> R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

[Footnote added.]

CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5, and R1.6 each have a "Medium" VRF and a "Severe" Violation Severity Level (VSL). CIP-006-1 R1.7, R1.8, and R1.9 each have a "Lower" VRF.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-006-1 R1. Specifically, URE reported that during an on-site assessment conducted by an external vendor, the vendor observed that there was an openly accessible human machine interface (HMI), classified as a Critical Cyber Asset (CCA), on the exterior wall of a Physical Security Perimeter (PSP). The HMI is a touch screen monitor allowing for local control of equipment. These HMIs communicate with programmable logic controllers (PLCs). Upon further examination, URE identified that this situation also existed at three other identically designed facilities. WECC determined that URE failed to provide a completely enclosed six-wall border to eight CCAs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE removed the HMI monitors from service.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs had 24 hour a day, seven day a week physical and electronic monitoring and alarming. URE's control rooms are manned continuously and the control room operator monitor alerts regarding any unexpected activity at the HMIs. In the event that an HMI is compromised, alarms immediately notify personnel responsible for response. In addition, the devices have a restrictive operating system that limits physical access at the face of the devices.

CIP-006-3a R5
CIP-006-3a R5 provides:

> R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:
>
> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
>
> • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

CIP-006-3a R5 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-006-3c R5. Specifically, URE reported six incidents where it failed to implement its technical and procedural controls for monitoring physical access at access points to the PSPs 24 hours a day, seven days a week:

1. For approximately two hours, URE's physical access control and monitoring (PACM) server failed and was not actively monitoring logs sent from the physical access points to six PSPs;
2. For approximately one hour, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to six of its PSPs;
3. For approximately ten minutes, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to six of its PSPs;
4. For approximately four hours, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to four of its PSPs;
5. For approximately two hours, URE's PACM server failed and was not actively monitoring logs sent from the physical access points to four of its PSPs; and
6. A URE system operator disarmed a PSP's two access points but failed to re-arm the access points when finished, resulting in a failure to provide access monitoring for 17 hours.

WECC determined the duration of the violation to be from the date on which URE first failed to implement the controls for monitoring access at all access points to the PSPs, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to monitor physical access at all access points to the PSPs could allow unauthorized access to the PSP to go unnoticed and unchecked, potentially allowing malicious access to Cyber Assets. Individuals could then use such access to cause harm to CCAs essential to the operation of the BPS.

The five instances where the PACM server failed were unplanned, and ranged from ten minutes to four hours. This reduced the likelihood that a malicious actor would know of the outages and have the opportunity to gain malicious access to Cyber Assets. For the sixth instance, the PSP resided in a secure facility where physical access is monitored and restricted by use of a card key. Therefore, even though the specific cabinet and CCA were not re-armed, there were still only a select few individuals with access to the room where the cabinet was housed, and the CCA required appropriate credentials to gain access. Accordingly, even though the drawer was unlocked and unarmed, a malicious actor would require appropriate logical credentials to access the drawer.

CIP-007

The purpose statement of Reliability Standard CIP-007 provides:

> Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-007-1 R2

CIP-007-1 R2 provides:

> Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-007-1 R2. Specifically, URE reported it did not adequately evaluate the ports and services to determine whether it had enabled only those ports and services required for normal and emergency operations for Cyber Assets located at six locations.

Initially, URE documented a baseline of all open ports on its system. This baseline was determined based on URE's review of vendor documentation describing expected ports to be open related to running services. However, this review failed to evaluate effectively and document the need for ports and services not identified by the vendor as a potential threat to security. URE identified 19 ports that were enabled without documenting whether they were required for normal and emergency operations. WECC determined that URE failed to establish, document, and implement a process to ensure that it only enabled those ports and services required for normal and emergency operations.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The ports were identified applications on devices that were all located within an Electronic Security Perimeter (ESP). In addition, URE monitors all logical access, and protective boundary devices restrict access. The devices in scope have antivirus and malware prevention tools installed. Finally, URE was aware the 19 ports were open and was actively monitoring the use of the ports.

CIP-007-1 R3

CIP-007-1 R3 provides:

> Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-007-1 R3. Specifically, URE reported it failed to apply its patch management program to certain devices located within the ESPs at its facilities. URE failed to track, evaluate, and install 46 security patches released that were applicable to 24 networking devices. Additionally, it failed to track patches for 78 devices comprised of PLCs, emission analyzers, global positioning system (GPS) clocks, chart recorders, thin clients, protocol converters, and switches. WECC determined that because URE was not performing any type of patch tracking on these devices, URE had no way of knowing if or when a patch was released.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to assess security patches could result in vulnerabilities remaining unaddressed for extended periods. This increases the risk of a successful

cyber-attack against CCAs. This increased risk may allow for unauthorized internal and or external access, which could allow for successful cyber-attacks against CCAs essential to operation of the BPS.

Although URE failed to make documentation and records of its security patches available, the devices in scope were all located within an ESP, URE monitored access, and protective boundary devices restricted access. URE stated that the devices in scope have antivirus and malware prevention tools installed and backup procedures in place to limit the duration and exposure of an outage or malicious activity caused by not keeping up to date on patch management.

CIP-007-1 R6

CIP-007-1 R6 provides:

> Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
>
> R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
>
> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Certification to WECC addressing noncompliance with CIP-007-1 R6. Specifically, URE reported it failed to implement automated tools or organizational process controls to monitor cyber security system events for 83 Cyber Assets within an ESP. URE stated it was unsure if the 83 devices were capable of logging.

WECC determined that URE failed to implement automated tools or organizational process controls to monitor system events related to cyber security for Cyber Assets within the ESP. The 83 devices in scope consisted of PLCs, emission analyzers, GPS clocks, chart recorders, thin clients, and protocol converters, which were not logging access as required.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All the devices are located within an ESP, URE monitors access, and protective boundary devices restrict access. URE stated that the devices in scope have antivirus and malware prevention tools installed where technically feasible, and backup procedures are in place to limit the duration and exposure of an outage or malicious activity.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred nine thousand dollars ($109,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered certain prior violations in URE's compliance history as aggravating factors in penalty determination;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had an internal compliance program (ICP) at the time of the violations which WECC considered a mitigating factor;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-006-1 R1, CIP-007-1 R2, and CIP-007-1 R6 posed a minimal risk to the reliability of the BPS, and the violations of CIP-006-3a R5 and CIP-007-1 R3 posed a moderate risk to the reliability of the BPS, as discussed above;

6. URE submitted to WECC a narrative describing compliance-related improvements URE has made. WECC will review URE's submission and may elect to provide feedback to URE;[5] and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred nine thousand dollars ($109,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-006-1 R1
URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC as complete. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT008701 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the HMI monitors from service by disconnecting the Ethernet communications and power sources;
2. change the connection method from Ethernet connections to serial connections, thereby removing these devices from the scope of the NERC CIP Standards; and
3. remove the HMI devices from its CCA list.

URE certified that the above Mitigation Plan requirements were completed.

[5] The narrative described how URE implemented the following changes: 1) URE has developed a process to track deadlines and mitigate violations in a timely manner, thereby minimizing the need for extension requests; 2) URE has created a monthly coordination meeting between compliance groups. This meeting focuses on increasing communication between entities and centralizing issues stemming from information silos; 3) URE has created an annual compliance awareness training program to measure the degree of understanding. URE will include a section to prevent recurrence of NERC Reliability Standard violations; and 4) URE has developed either a process, or improvements to processes, that will help identify the full scope of violations promptly. URE will develop a process for detecting what controls are needed when new devices are installed.
[6] *See* 18 C.F.R § 39.7(d)(7).

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-006-3a R5

URE's Mitigation Plan to address its violation of CIP-006-3a R5 was submitted to WECC as complete. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT009130 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revise its physical security plan to address unplanned PACM server outages;
2. develop a new procedure to address unscheduled outages;
3. upgrade the PACM system to enable functional hardware redundancy;
4. add procedural controls and requirements for rearming all PSP doors and cabinets and responding during an unscheduled outage; and
5. repair the failed power supply drive and return the system to service.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT009047 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the ports and services procedure and toolkit. This process includes the following:
    a. work with the vendor to determine the required ports and services;
    b. monitor system operation;
    c. document ports;

d. scan devices to find open/enabled ports;

e. compare results.

2. determine if any unused ports and services require a Technical Feasibility Exception (TFE).

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT009048 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a new patch management program and bring patches and security updates to the latest releases; and
2. hold employee workshops and informal discussions to review procedures to let personnel know that patches are applicable to all Cyber Assets within the ESP and not just CCAs.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT009049-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a checklist for all assets to determine if the device is capable of logging or if a TFE is needed;
2. perform an assessment of all assets and document what devices are capable of logging to URE's security information and event management database; and

3. file any necessary TFEs.

URE certified that the above Mitigation Plan requirements were completed.

After WECC's review of URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on January 14, 2014. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred nine thousand dollar ($109,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. WECC considered certain prior violations in URE's compliance history as aggravating factors in penalty determination, as discussed above;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had an ICP at the time of the violations which WECC considered a mitigating factor, as discussed above;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-006-1 R1, CIP-007-1 R2, and CIP-007-1 R6 posed a minimal risk to the reliability of the BPS, and the violations of CIP-006-3a and CIP-007-1 R3 posed a moderate risk to the reliability of the BPS, as discussed above;

[7] *See* 18 C.F.R. § 39.7(d)(4).
[8] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

6. URE submitted a narrative to WECC describing compliance-related improvements, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred nine thousand dollars ($109,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between WECC and URE, included as Attachment a;

b) Record documents for the violation of CIP-006-1 R1, included as Attachment b:
   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT008701;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-006-3a R5, included as Attachment c:
   1. URE's Source Document;
   2. URE's Mitigation Plan designated as WECCMIT009130;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-007-1 R2, included as Attachment d:
   1. URE's Source Document;

2. URE's Mitigation Plan designated as WECCMIT009047;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-007-1 R3, included as Attachment e:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT009048;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion;
5. WECC's Verification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-007-1 R6, included as Attachment f:

1. URE's Source Document;
2. URE's Mitigation Plan designated as WECCMIT009049-2;
3. URE's Mitigation Plan Extension Request;
4. URE's Certification of Mitigation Plan Completion; and
5. WECC's Verification of Mitigation Plan Completion.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 N. 400 W. Suite 200 Salt Lake City, UT 84103 801-883-6853 jrobb@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz

Chris Luras* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Assistant General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
North American Electric Reliability Corporation
Senior Counsel and Associate Director, Enforcement Processing
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

January 30, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP14-29-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Reliability*First* Corporation (Reliability*First*) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First*'s determination and findings of the violations[3] of CIP-005-1, CIP-005-3a, CIP-005-3, CIP-006-1, CIP-007-1, and CIP-007-3. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventy-five thousand dollars ($75,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC2013011941, RFC2013012708, RFC2012011452, RFC2012011455, RFC2012011568,

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

RFC2012011569, RFC2013012114, RFC2013011942, RFC2013011943, RFC2013011945, RFC2012011453, RFC2012011454, and RFC2013013118 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between Reliability*First* and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Reliability*First* Corporation	Unidentified Registered Entity	NOC-2261	RFC2013011941	CIP-005-1	R2; R2.2	Medium	$75,000
			RFC2013012708	CIP-005-3a	R3; R3.2	Medium	
			RFC2012011452	CIP-005-3	R4	Medium	
			RFC2012011455	CIP-007-3	R8	Lower	
			RFC2012011568	CIP-006-1	R1	Medium	
			RFC2012011569	CIP-006-1	R2; R2.2	Medium	
			RFC2013012114	CIP-007-1	R1; R1.1	Medium	
			RFC2013011942	CIP-007-1	R2	Medium	
			RFC2013011943	CIP-007-1	R3	Lower	

			RFC2013011945	CIP-007-1	R4; R4.2	Medium	
			RFC2012011453	CIP-007-1	R5; R5.2	Lower	
			RFC2012011454	CIP-007-1	R6; R6.3, R6.4, R6.5	Medium	
			RFC2013013118	CIP-007-1	R6; R6.3, R6.4, R6.5	Medium	

CIP-005-1 R2; R2.2 (RFC2013011941)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ***
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> ***

CIP-005-1 R2 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-005-1 R2. During a Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-005-1 R2.

During URE's cyber vulnerability assessment (CVA), it performs a detailed ports and services assessment to ensure that only those ports and services necessary for secure operation are enabled. The resulting annual CVA then becomes the new baseline for ports and services. URE did not maintain this baseline configuration between annual CVAs. Instead, it restarted the baseline each year, meaning ports and services could have been modified without authorization since the last CVA without detection.

URE's document listing the ports and services does not document or tie the ports and services to individual assets or specified groupings to identify which ports and services should be enabled on which devices or device types. For at least one switch, certain ports were enabled but not listed as such in URE's document. In addition, there were three ports and services that were enabled that were not required for normal or emergency operations.

Reliability*First* determined that URE had a violation of CIP-005-1 R2 because it failed to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter (ESP).

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect Electronic Security Perimeter (ESP) access points increases the likelihood of a gap in security defenses for the ESP. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Although URE did not maintain a baseline between CVAs, each change to ports and services required prior approval through the change control process. In addition, the annual CVA change ticket assessments and the ports and services true-ups have not identified any unauthorized enabled ports and services. Regarding the issue, the devices at issue are located within an ESP and a Physical Security Perimeter (PSP). This means additional credentials are required to gain access to the devices, the site has restricted physical access, and the site is manned at all times. In addition, URE review of the open ports and services demonstrated that all but three of its open ports and services were required.

CIP-005-3a R3; R3.2 (RFC2013012708)

The purpose statement of Reliability Standard CIP-005-3a R3 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a R3 provides in pertinent part:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> ***
>
> R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-3a R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-005-3a R3. During a daily review, URE discovered that the process syslog collector was not running on the electronic security manager. The file system filled up due to stoppage of the process parsetext collector. As a result, there were the three gaps for over 10 hours in logging on certain electronic access control and monitoring devices.

Reliability*First* determined that URE had a violation of CIP-005-3a R3 because it failed to implement its electronic process for monitoring and logging access at access points to the ESP at all times.

Reliability*First* determined the duration of the violation to be from the date the file system stopped collecting logs, through the present.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, missing logs increase the likelihood of undetected

and unauthorized access to URE's system. The risk to the reliability of the BPS was mitigated by the following factors. The gap in logs impacted a limited number of devices. For the duration of the violation, there were no cyber security incidents on URE's monitored equipment.

CIP-005-3 R4 (RFC2012011452) and CIP-007-3 R8 (RFC2012011455)

The purpose statement of Reliability Standard CIP-005-3 provides in pertinent part: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-3 R4 provides:

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings;
>
> R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-3 provides in pertinent part: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-3 R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
>
> R8.3. A review of controls for default accounts; and,
>
> R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-3 has a "Medium" VRF and a "Severe" VSL.

URE submitted Self-Reports to Reliability*First* stating that it was in violation of CIP-005-3 R4 and CIP-007-3 R8. URE submitted another Self-Report to Reliability*First* stating that it was in violation of CIP-005-3 R4. During the Compliance Audit, Reliability*First* discovered additional violations of CIP-005-3a R4 and CIP-007-3 R8.

URE performed CVAs for two consecutive years for its electronic access points to the ESP and Cyber Assets within the ESP, but did not have an adequately defined process for performing CVAs. In addition, URE failed to have documentation demonstrating that it included all the following requirements of CIP-005-3 R4 and CIP-007-3 R8 in its CVA: 1) a document identifying the CVA process (CIP-005-3a R4.1 and CIP-007-3 R8.1); 2) a review to verify that it enabled only ports and services required for operations at access points to the ESP (CIP-005-3a R4.2) and for Cyber Assets within the ESP (CIP-007-3 R8.2); 3) the discovery of all access points to the ESP (CIP-005-3a R4.3); 4) a review of controls for default accounts (CIP-005-3a R4.4 and CIP-007-3 R8.3); 5) passwords and network management community strings[4] (CIP-005-3a R4.4); and 6) documentation of the results of the

[4] Community strings are similar to a user identification or password that allows access to a router's or other device's statistics.

assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan (CIP-005-3a R4.5 and CIP-007-3 R8.5).

URE performed CVAs for two consecutive years but failed to conduct a review of controls for network community strings, as required by CIP-005-3a R4.4.

Reliability*First* determined that URE had a violation of CIP-005-3 R4 because it failed to include in its CVA: 1) the required elements for electronic access points to the ESP; and 2) a review of controls for network management community strings. Reliability*First* determined that URE had a violation of CIP-007-3 R8 because it failed to include the required elements in its CVA for Cyber Assets within the ESP.

Reliability*First* determined the duration of the violations to be from the date by which URE was required to conduct a CVA through when URE completed its Mitigation Plan.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to define and execute an adequate CVA increases the likelihood of compromise to the assets subject to the CVAs. In addition, the lengthy duration of the violation, over two years, increased URE's exposure to this risk.

The risk to the reliability of the BPS was mitigated by the following factors. URE did perform the CVA, and the individuals who performed the assessments can provide supporting details of those assessments. This was a documentation issue where URE failed to retain documentation supporting those details. In addition, for several years, URE configured all access points' network management community strings to be unidirectional (read-only). Furthermore, URE did not use the default values (public or private) for the network management community strings. URE restricted them so they were only accessible by specific internal Cyber Assets, and URE updated them to the latest version.

CIP-006-1 R1; R1.1 (RFC2012011568)

The purpose statement of Reliability Standard CIP-006-1 R1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R1. URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R1. Reliability*First* consolidated the two instances of noncompliance into RFC2012011568. First, URE discovered a five-foot by 18-inch opening in the six-wall border above the suspended ceiling of a PSP at a generating facility. Second, URE maintains one ESP at a generating station with assets in multiple PSPs. URE discovered that the wiring connecting the Cyber Assets in discrete PSPs is not protected by a six-wall boundary such as conduit. URE submitted a Technical Feasibility Exception (TFE) for this issue, which was approved.

Reliability*First* determined that URE had a violation of CIP-006-1 R1 because it failed to ensure all Cyber Assets within an ESP reside within an identified PSP.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Regarding the gap in the six-wall border, there are additional protections in place for the CCAs. The gap in the PSP would only allow access to a hallway within the PSP where no CCAs reside. In order to access the CCAs, an individual would need to access an additional door with a card reader. Regarding the exposed wiring, the assets and the wiring are located within a restricted access site that is manned 24 hours a day. In addition, URE has cameras in place, as well as physical personnel presence, for monitoring of the site at all times.

CIP-006-1 R2; R2.2 (RFC2012011569)
CIP-006-1 R2 provides in pertinent part:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> ***
>
> R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
>
> ***

CIP-006-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R2. URE submitted another Self-Report to Reliability*First* stating that it was in violation of CIP-006-1 R2. Reliability*First* incorporated both instances of noncompliance into RFC2012011569.

URE discovered that it did not identify its physical access control system (PACS) intelligent controllers as Cyber Assets that authorize and/or log access to the PSP. As a result, URE failed to provide certain protective measures to these devices, as required by CIP-006-1 R2.2. URE also failed to provide the protective measures of CIP-003 R6, CIP-004 R3 and R4, CIP-007, CIP-008, and CIP-009.

In addition, URE installed two servers, which are Cyber Assets that authorize and/or log access to the PSP. URE failed to afford the protective measures of CIP-007-3 R6 to these devices by failing to install the required logging and monitoring software agent on these servers. URE enabled the devices to log all possible events, which resulted in a large number of events generated on these servers. Because URE did not install the required software agent, the logs were being overwritten in less than 24 hours, so URE was unable to review the logs manually. As a result, these servers did not provide security logs for URE's review, and URE did not retain these logs for 90 calendar days, as required by CIP-007-3 R6.

Reliability*First* determined that URE had a violation of CIP-006-1 R2 because it failed to afford certain protective measures to Cyber Assets that authorize and/or log access to the PSP.

Reliability*First* determined the duration of the first instance of the violation to be from the date URE was required to comply with CIP-006-2 for the PACS intelligent controllers, through when URE completed its Mitigation Plan. Reliability*First* determined the duration of the second instance of the violation to be from the date URE installed the servers, through the date URE installed logging and monitoring software.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect the system intelligent controllers increased the likelihood of compromise of the administrative workstation. Also, failure to protect the servers increased the likelihood of an undetected incident. Furthermore, the duration of the violation increased URE's exposure to this risk. The risk to the BPS was mitigated by the following factors. Regarding the logging and monitoring software on the servers, the PACS has additional network-based monitoring systems in place that log network activity such as the intrusion detection system and the PACS network access point firewalls, all of which send their logs to the security information and event management system where security analysts monitor them. Unauthorized traffic would have had to bypass the intrusion detection system and the firewalls prior to attempting to compromise the servers. In addition, both servers had the required malware prevention software installed. This software reports threats to the enterprise malware prevention console software which, in turn, sends the events to the security information and event management system.

CIP-007-1 R1; R1.1 (RFC2013012114)

The purpose statement of Reliability Standard CIP-007-1 R1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-1 R1 provides in pertinent part:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

***

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, Reliability*First* discovered that URE had a violation of CIP-007-1 R1. Reliability*First* determined that URE's cyber security test procedures for new Cyber Assets and significant changes to existing Cyber Assets within the ESP were inadequate. For example, the test plan descriptions and results of testing did not reflect testing of cyber security controls. In addition, URE had change control tickets documenting that testing personnel answered certain questions during the change process, but URE did not provide evidence that the testing prevented adverse effects on cyber security controls. As a result, URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls.

In addition, Reliability*First* determined that URE conducted cyber security testing for software changes or upgrades in the production environment utilizing an approach that does not minimize adverse effects on the production environment. URE, using the "rolling wave" method, performed cyber security testing for software changes and upgrades on the assets that are less critical first, followed by a time period (usually 24 hours) to verify successful deployment prior to continuing deployment to assets that are more critical. This approach did not adequately minimize adverse effects on the production system or its operation, as required by CIP-007-3 R1.1, because untested upgrades may contaminate the environment.

Reliability*First* determined that URE had a violation of CIP-007-1 R1 because URE failed to: 1) ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls; and 2) implement cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of BPS, but did not pose a serious or substantial risk. Specifically, testing security controls on a CCA after making a change to the system is crucial. Without such testing, the change to the system could introduce an unknown vulnerability to the system. In addition, the lengthy duration of the violation increased URE's exposure

to this risk. The risk to the reliability of the BPS was mitigated by the following factors. URE's process made the change approvers aware of the impact the change would have and allowed them to approve or deny the change request accordingly. In addition, URE used a process where any changes to firewall rules required the justification to be added as a comment to the rule set along with a reference to the associated change ticket number. URE also leveraged the annual CVA process to test all cyber security controls and confirm that it had documented any changes since the prior year through change tickets. As a result, although URE's change control process was inadequate, URE had a functioning change control process.

In addition, the ESP and PACS environments have additional network-based monitoring systems in place that log network activity, such as the intrusion detection system (IDS) and network access point firewalls, all of which send their logs to the security monitoring system where security analysts monitor them. Any undetected compromise of these systems would have had to bypass the IDS and the firewalls prior to attempting to compromise Cyber Assets within these environments. All URE's operating system servers and workstations have the required malware prevention software installed. The malware prevention software is configured to report threats to the enterprise malware prevention console software, which in turn sends the events to the security monitoring system. All devices in these environments have security patches applied in accordance with the URE patch management program. Furthermore, URE's vendor tests for functionality issues and only provides updates that pass its testing process. URE has not experienced any security issues resulting from the "rolling wave" approach.

CIP-007-1 R2 (RFC2013011942)

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-1 R2. During the Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-007-1 R2 for URE. During URE's CVA, URE performs a detailed ports and services assessment to ensure that only those ports and services necessary for secure operation are enabled. The resulting annual CVA becomes the new baseline for ports and services. However, URE did not maintain this baseline configuration between annual CVAs. As a result, ports and services could have been modified without authorization since the last cyber CVA without detection since URE restarts the baseline each year.

During URE's CVA for a specific year, URE identified that several of its open ports and services were not justified as being required for normal and emergency operations. URE discovered these open ports and services because the third-party contractor that performed URE's CVA utilized an improved tool. For the majority of the open ports and services, URE obtained justification that they were required for normal and emergency operations. URE has documented confirmation that it should disable seven of these open ports and services.

In addition, URE's list of ports and services did not document individually or by specified grouping which ports and services should be enabled or listening on which devices.

Reliability*First* determined that URE had a violation of CIP-007-1 R2 because it failed to implement its process to ensure that only those ports and services required for normal and emergency operations are enabled as related to securing those systems determined to be CCAs.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, to the present.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to protect Cyber Assets within the ESP through a ports and services baseline increases the likelihood of a security gap. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the BPS was mitigated by the following factors. Although URE failed to maintain the ports and services baselines, each change to ports and services required prior approval through the change control process. URE utilized these

change tickets to request, authorize, and document ports and services changes between CVAs. The annual CVA change ticket assessments did not identify any unauthorized enabled ports and services. In addition, URE's change control process included questions related to the impact on ports and services for a given change, and allowed approvers to approve or deny the change request accordingly.

Furthermore, the ESP and PACs environments have additional network-based monitoring systems in place that log network activity, such as the IDS and network access point firewalls, all of which send their logs to the security monitoring system where security analysts monitor them. Any undetected compromise of these systems would have had to bypass the IDS and the firewalls prior to attempting to compromise Cyber Assets within these environments. All Windows servers and workstations have the required malware prevention software installed. The malware prevention software is configured to report threats to the enterprise malware prevention console software, which in turn sends the events to the security monitoring system. All devices in these environments have security patches applied in accordance with the URE patch management program.

Regarding URE's open ports and services, the devices are not connected to the business local area network or the Internet. The devices were all located within an ESP and PSP with an additional firewall present between the devices and URE's system, and as a result, extra credentials were required to access these devices.

CIP-007-1 R3 (RFC2013011943)

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R3. During the Compliance Audit, Reliability*First* discovered an additional instance of a violation of CIP-007-1 R3 for URE. URE evaluated security patches released from its vendor within 30 days of release from the vendor. However, URE should have been assessing security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades from the application vendor. In addition, URE provided insufficient evidence that its vendor was in fact performing assessments of these patches. Instead, URE provided evidence that its vendor was testing the patches but not assessing them for applicability.

In addition, Reliability*First* discovered that URE's security patch implementation did not address software patch updates beyond security patches for certain software. For example, URE does not assess and implement security patches.

Reliability*First* determined that URE had a violation of CIP-007-1 R3 because it failed to implement its security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches.

Reliability*First* determined the duration of the violation to be from the date by which URE was required to comply with CIP-007-1 through when URE completed its Mitigation Plan.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to document the assessment of security patches and upgrades increases the likelihood of inadequately protecting Cyber Assets. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Regarding URE's assessment of security patches, URE performed assessments of security patches, although at an interval greater than 30 days. In addition, the devices were all located within an ESP and PSP, and as a result, extra credentials were required to access these devices.

Regarding URE's security patch implementation, the accounts at issue do not have direct outward facing access to the corporate business network or to the Internet, reducing the likelihood of access from outside the network.

CIP-007-1 R4 (RFC2013011945)

CIP-007-1 R4 provides in pertinent part:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> ***
>
> R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R4. The anti-virus and malware prevention signatures on URE's voltage regulators for its generating stations were not up to date or available, as required by CIP-007-3 R4.2. Although these voltage regulators are technically incapable of running anti-virus and malware prevention tools, URE failed to submit a TFE.

During the Compliance Audit, Reliability*First* discovered an additional instance of non-compliance with CIP-007-1 R4 for URE. Reliability*First* discovered that URE , using the "rolling wave" approach, performs testing and implementing for updated signature files on the assets that are less critical first, followed by a time period (usually 24 hours) to verify successful deployment prior to continuing deployment to assets that are more critical. This approach places the signatures into the production environment prior to testing, and as such does not adequately address testing of anti-virus and malware prevention signatures, as required by CIP-007-3 R4.2.

Reliability*First* determined that URE had a violation of CIP-007-1 R4 because it failed to: 1) implement its process for testing anti-virus and malware preventions signatures; and 2) implement its process for the update of anti-virus and malware prevention signatures.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of BPS, but did not pose a serious or substantial risk. Specifically, the "rolling wave" approach increases the likelihood of compromise to Cyber Assets within the production environment. In addition, the lengthy duration of the violation increased URE's exposure to this risk. The risk to the reliability of the BPS was mitigated by the following factors. Regarding the voltage regulator devices, the devices are located within an ESP and PSP and additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned at all times. Regarding testing of the signatures, URE installed anti-virus software and has not experienced any security issues resulting from the "rolling wave" approach.

CIP-007-1 R5 (RFC2012011453)

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> ***
>
> R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
>
> > R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.
> >
> > R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.
> >
> > R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).
>
> ***

CIP-007-1 R5 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R5. For one shared account, URE limited access to three individuals who typically use their own separate laptop to log into the account. URE traced the usage of the shared account through the unique IP address of the specific user. However, URE discovered that a user may access another user's laptop to log into the account, thereby rendering the account use untraceable. Therefore, URE failed to implement an audit trail of the account use for this account, as required by CIP-007-3 R5.2.3.

URE submitted a Self-Report to Reliability*First* stating that it was in violation of CIP-007-3 R5. Specifically, URE does not have evidence of audit trails of individual user account activity for its generating station voltage regulators. For certain devices, URE did not review logs, and for other devices, such logs are unavailable. Therefore, URE failed to implement its policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts, as required by CIP-007-3 R5.2.

During the Compliance Audit, Reliability*First* discovered another instance of non-compliance with CIP-007-3 R5. Reliability*First* discovered that for several shared accounts that URE could have renamed, URE failed to do so, as required by CIP-007-3 R5.2.1. For example, URE failed to rename the administrator accounts for certain devices. In addition, Reliability*First* discovered that URE could not provide sufficient evidence of individual access to shared accounts, as required by CIP-007-3 R5.2.2.

Reliability*First* determined that URE had a violation of CIP-007-3 R5 because it failed to: 1) establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of certain individual user account access activity for a minimum of 90 days; 2) implement its policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts; and 3) have in place an audit trail of the account use for one shared account.

Reliability*First* determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the present.

Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to rename administrator accounts poses a risk to the reliability of the BPS by providing a potential intruder with part of the login information to an account that can perform administrator tasks on the system. This increases the likelihood of compromise to BPS reliability. The risk to the reliability of the BPS was mitigated by the following factors. Regarding the failure to rename administrator accounts, the accounts at issue do not have direct outward facing access to the corporate business network or to the internet, reducing the

likelihood of access from outside the network. URE restricts all physical access to Cyber Assets to individuals with valid personnel risk assessments (PRAs) and annual cyber security training.

Regarding the voltage regulator devices, the devices are located within an ESP and PSP, which means additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned at all times.

Regarding the audit trail of the shared account, the three individuals had authorized access to the shared account and had valid PRAs and cyber security training during the time period of the violation. In addition, URE experienced no cyber security events during the time period of the violation, and URE did not need to call upon the audit trail for this account.

CIP-007-1 R6; R6.3, R6.4, R6.5 (RFC2012011454 and RFC2013013118)

CIP-007-1 R6 provides in pertinent part:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
> >
> > R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
> >
> > R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (RFC2012011454). Specifically, URE discovered that monitoring was temporarily disabled on five Cyber Assets within the ESP.

During the Compliance Audit, Reliability*First* discovered that URE had several devices configured to the security information and event management system that were technically incapable of performing monitoring or generating logs. URE failed to submit a TFE for these devices.

URE submitted another Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (RFC2013013118). During a routine log review, URE discovered that the collection Internet Protocol address for one aggregate switch was misconfigured. As a result, URE failed to review logging for the switch due to lack of log data.

URE submitted another Self-Report to Reliability*First* stating it was in violation of CIP-007-3 R6 (consolidated into RFC2013013118). During an unplanned outage of URE's security manager security information and event management tool, URE discovered that for several devices, messages pertaining to denied firewall traffic were not collected because of the inadequacy of the frequency at which log buffers can send logging information to a collection device.

Reliability*First* determined that URE had a violation of CIP-007-1 R6 because it failed to monitor continuously the activity on all its Cyber Assets or submit a TFE where appropriate.

Reliability*First* determined the duration of the violation RFC2012011454 to be from when URE was required to submit a TFE through when URE completed its Mitigation Plan. Reliability*First* determined the duration of the violation RFC2013013118 to be from the date the Standard became mandatory and enforceable on URE through the present.

Reliability*First* determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the separate instances of noncompliance making up this violation resulted in multiple vulnerabilities on URE's system. The risk to the reliability of the BPS was mitigated by the following factors. URE controls physical access to the devices through a key management program. URE had the following security measures in place: 1) the cabinet doors that contain the devices are protected by alarm, and URE security personnel monitors them 24 hours a day; 2) all personnel with physical and/or logical access have valid PRAs and cyber security training; 3) the single default local administrator account is disabled; 4) the devices are physically stored in a controlled access PSP, and network intrusion detection is active and monitoring for anomalous traffic; 5) URE's passwords for these devices meet or exceed the CIP password complexity and change requirements; and 6) URE has installed, maintained, and monitored anti-virus on all operating system servers and workstations.

Regarding the voltage regulator devices, the devices are located within an ESP and PSP, and additional credentials are required to gain access to this device. In addition, the site has restricted access and is manned 24 hours a day. Regarding the aggregate switch, URE's system segments traffic from the aggregate switch feeder systems, which gather data to be published as view-only on the server. As a result, the loss of this traffic does not affect BPS operation. Regarding the affected devices, the loss of logging information does not directly affect BPS operation but instead provides insight into the traffic flowing across the network.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Reliability*First* has assessed a penalty of seventy-five thousand dollars ($75,000) for the referenced violations. In reaching this determination, Reliability*First* considered the following factors:

1. URE's violation history, which was considered an aggravating factor in penalty assessment;
2. URE self-reported the violations, except for the CIP-007-1 R1.1 violation;[5]
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE committed to performing above-and-beyond activities to implement reliability enhancements that exceed those actions that would achieve and maintain baseline compliance with the NERC CIP Reliability Standards and Requirements, as described below;
8. When considered as an aggregate, the instant violations posed an elevated level of possible risk to URE's Cyber Assets, which was indicative of programmatic failure; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[5]URE historically engages in rigorous self-assessments, the result of which are robust Self-Reports and rigorous mitigating activities. While URE failed to timely detect many of these issues, URE's historic compliance performance demonstrates its commitment to spontaneous timely detection and timely correction unconnected to a pending regional compliance monitoring action.

URE committed to collaborating with Reliability*First* to perform the following above-and-beyond activities to implement reliability enhancements. Specifically, URE agreed to perform certain actions to improve its capability and performance in key management practices of asset and configuration management, verification, and validation.

Based on information provided by URE throughout the Compliance Audit and enforcement process, Reliability*First* analyzed the root cause and risk severity of the instant violations and determined that if URE had high capability and performance in certain key management practices, the number and severity of URE's violations may have been reduced. First, high capability and performance in asset and configuration management would impact compliance with many of the Requirements at issue in the violations. When implementing asset and configuration management programs, entities establish an inventory of assets and configurable items, define the attributes of those assets and configurable items, and maintain their integrity in the context of reliability and resilience. The violations impacted by these activities are the violations related to asset identification (CIP-006 R2.2), CVAs (CIP-005 R4 and CIP-007 R8), and Cyber Asset change control and configuration management (CIP-005 R2.2 and CIP-007 R1, R3, R4 R5, and R6).

Second, high capability and performance in validation and verification activities would impact compliance with many of the Requirements at issue in the violations. Validation activities confirm that changes to the systems comprising the BPS function as designed in the intended environment and conditions before the changes are made operational. Verification activities confirm that any changes to the systems comprising the BPS and affecting its reliability are conducted in accordance with requirements, plans, or specifications. URE performed cyber security functions separately for its affected and business units, which resulted in numerous violations (CIP-005 R2 and R4 and CIP-007 R1, R2, R3, R4, R5, and R8). These violations include processes that involve the testing and validation of electronic access, software upgrades, secure ports and services, patch updates, malware updates, valid accounts, and properly assessed cyber vulnerabilities. All of these are testing and validation processes, thereby demonstrating improvement opportunities in validation and verification.

These key management practice areas (asset and configuration management, validation, and verification) are correctly mapped to the root causes of the identified violations and constitute areas for improvement. URE completed the mitigating actions set forth below for each violation, and those mitigating actions resulted in a baseline level of internal controls sufficient to return URE to compliance with the Requirements at present and prevent recurrence of the same noncompliance. However, URE and Reliability*First* determined that improving URE's capability and performance in the identified key management practices would lead to improved grid reliability and resilience and institute a higher level

of preventative internal controls that may further prevent noncompliance with a wider array of Requirements.

To that end, URE agreed to collaborate with Reliability*First* to undertake the actions set forth below in order to improve its capability and performance in these key management practices of asset and configuration management, verification, and validation. Such process improvements, when fully implemented, will positively impact compliance with the Requirements that constitute the majority of the violations at issue in this Agreement and will result in holistic improvement to grid reliability and resiliency.

By analyzing the root causes of its violations and surveying available frameworks, URE agreed to utilize the SANS Institute's 20 Critical Controls for Effective Cyber Defense (SANS 20) in effect at the time of the Settlement Agreement, to develop and implement an internal controls framework related to frequently-violated, high-risk Requirements. The SANS 20 are critical controls for effective cyber defense, developed originally by the National Security Agency (NSA) and the SANS Institute to "share [the NSA's] attack information to provide … control-prioritization knowledge for civilian government agencies and critical infrastructure."[6] The SANS 20 methodology is a "living" document that changes based on the most relevant threat information identified by multiple experts and agencies and based on actual attacks and effective defenses.[7]

The SANS 20 supports cyber security and reliability capability and performance, and its goals align with the goals of the CIP Requirements as well as asset and configuration management. The goal of the SANS 20 is to "protect critical assets, infrastructure, and information by strengthening [an] organization's defensive posture through continuous, automated protection and monitoring of sensitive information technology infrastructure to reduce compromises, minimize the need for recovery efforts, and lower associated costs."[8] Similarly, the CIP Requirements aim to protect critical infrastructure by, among other things, implementing the continuous, automated protection and monitoring on high-value assets and configurable items, as described in the SANS 20 and identified by the asset and configuration management practice. Mapping the SANS 20 to the Requirements is therefore a worthwhile endeavor because it can assist URE and other Registered Entities with implementing robust cyber security that meaningfully impacts grid reliability. Rather than implementing an internal controls framework in a vacuum, or an internal controls framework related

[6] *A Brief History of the 20 Critical Cyber Controls*, available at http://www.sans.org/critical-securitycontrols/history.php.

[7] *Critical Controls for Effective Cyber Defense, Version 4.1* (March, 2013), available at http://www.sans.org/critical-security-controls/guidelines.php, at 2.

[8] *Id*.

to the CIP Requirements as they stand at a given point in time, URE will leverage the work of experienced agencies and organizations to improve grid reliability and resilience through robust cyber security.

In recognition of improvement opportunities in the asset and configuration management practice, URE will have documented risks and associated detective, corrective, and preventive internal controls to address three CIP Requirements related to asset and configuration management that URE has frequently violated and that represent high risk to the BPS (CIP-007-1 R1, R2, and R6). URE will provide its risk assessment methodology and the results of the risk assessment to Reliability*First*.

URE will include an analysis of the SANS 20 in its development and assessment of its internal control framework. URE will have provide a mapping between the SANS 20 and the CIP Requirements. URE will have develop, assess and test internal controls for CIP-007-1 R1, R2, and R6, and prioritized by risk to grid reliability the internal control is designed to mitigate. URE will provide quarterly updates to Reliability*First* regarding its development and implementation of the internal control framework. This assist visit will include assessment of the internal controls framework, its impact on grid reliability, and its impact on compliance with the identified Requirements.

Pursuant to URE's goal of improving its asset and configuration management especially related to CIP-007 R1, R2, and R6, Reliability*First* will conduct an assist visit with URE to review URE's capability and performance in asset and configuration management.

To focus on improvement opportunities in the validation and verification practices, URE is implementing a holistic approach to company-wide cyber security and reliability. In recognition that many of the violations resulted from divergent approaches to cyber security in various units, URE will implement a company-wide CIP program by integrating its divergent units' programs into one program. In addition, URE will put tools in place to improve its capability and performance in validation and verification of cyber security tasks important for grid reliability and resilience.

URE will implement a company-wide software tool that will assist with its validation and verification internal controls, including: 1) linkage to the internal controls framework (both a validation and verification activity); 2) reminders to perform periodic tasks (a verification activity); 3) awareness checks regarding activities related to Requirements (a validation activity); and 4) facilitation of compliance submittal management (a validation activity).

URE will evaluate the Mitigation Plans at issue in this Settlement Agreement to determine their alignment with the program. URE will provide Reliability*First* with a preliminary outline of reliability

risk areas relative to its CIP compliance program, capturing aspects of a risk assessment to be performed by a third-party consultant. Reliability*First* will provide feedback to URE regarding the outline, such that final scoping of the third-party risk assessment will be completed. URE will develop a plan to integrate all its business units' assets into one program to create a single, company-wide CIP program. In doing so, URE will undertake the integration by prioritizing its activities from highest to lowest risk to BPS reliability.

Reliability*First* and URE will work together to determine the scope of a Reliability*First*-led assist visit that will be most useful for URE to evaluate its company-wide CIP program. Reliability*First* will conduct an assist visit with URE to review URE's capability and performance in management practice areas related to the integration plan, including but not limited to validation and verification, to ensure their effectiveness for grid reliability and resilience. URE will provide Reliability*First* with an explanation of how it will incorporate the results from Reliability*First*'s assist visit and the third-party contractor's risk assessment into the implementation of its single company-wide CIP program. URE will complete the integration of the CIP program into the CIP program to create a single company-wide CIP program.

After consideration of the above factors, Reliability*First* determined that, in this instance, the penalty amount of seventy-five thousand dollars ($75,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[9]

CIP-005-1 R2 (RFC2013011941)
URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008835-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. define a dynamic ports and services process;
2. enhance its change control process;
3. issue documentation update;
4. perform training for relevant personnel;

[9] *See* 18 C.F.R § 39.7(d)(7).

5. aggregate running ports and services on devices at issue;
6. compile a list of unjustified ports and services;
7. obtain justification for or disable all unjustified ports and services;
8. disable any unjustified ports and services; and
9. update process documentation to include the ports and services methodology for justification of ports and services.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-005-3a R3; R3.2 (RFC2013012708)

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009920 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE Mitigation Plan requires URE to:

1. develop and implement system-compatible backup logging;
2. develop and document a process for maintenance and testing of the backup logging solution; and;
3. train applicable personnel on the process.

CIP-005-3a R4 (RFC2012011452)

URE's Mitigation Plan to address its violation of CIP-005-3a R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008887-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the CVAs at issue by hiring a third party that specializes in such assessments to conduct reviews;

2. update the CVA procedure to ensure the documented results align with each relevant CIP Requirement; and
3. update the vulnerability management program to include the missing network management community strings controls testing requirement.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R8 (RFC2012011455)

URE's Mitigation Plan to address its violation of CIP-007-3 R8 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008888-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the affected CVAs by hiring a third party that specializes in such assessments to conduct reviews;
2. update the CVA procedure to ensure the documented results align with each relevant CIP Requirement; and
3. update the vulnerability management program to include the missing network management community strings controls testing requirement.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-1 R1 (RFC2012011568)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009390 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. hire a construction firm to seal the opening above the suspended ceiling to the underside of the roof deck;
2. develop a preventative maintenance procedure for performing an annual assessment and to spot check boundaries periodically when there are construction activities in the area; and
3. submit a TFE for the issue with the exposed conduit.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-1 R2; R2.2 (RFC2012011569)

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009265-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an assessment and develop a document to identify the pertinent details for the intelligent controllers and associated information related to the PSP;
2. determine the technical capabilities of the intelligent controllers;
3. determine that it would submit TFEs for the intelligent controllers;
4. perform security capabilities testing on the intelligent controllers;
5. add the intelligent controllers associated with PSPs to the change and configuration management database;
6. update device configuration;
7. complete migration to the correct group at URE;
8. install the required logging and monitoring software agent on the servers; and
9. validate that both systems are sending all applicable security logs to the monitoring system.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-1 R1; R1.1 (RFC2013012114)

URE Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009538 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an exhaustive discovery of open ports and services, all accounts, Cyber Assets, applicable antivirus and malware signatures, and configuration baselines;
2. develop tools to automate discovery of local accounts, ports and services, registry settings, and simple network management protocol community strings;
3. define the scope of applicable security-related registry settings, and maintain monitoring of applicable security-related registry settings;
4. evaluate third-party vendor security testing for quality of evidence and test environment representative of production environment;
5. document the rolling wave approach and provide detail on devices in first wave and subsequent waves;
6. revise URE's procedure for process documentation to incorporate a cross-department peer review of CIP procedures;
7. commit to define dynamic ports and services process;
8. enhance the change control process;
9. issue documentation updates; and
10. perform communication and training to applicable personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R2 (RFC2013011942)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008836-3 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. implement a service contract to provide support for applicable devices;
2. implement the vendor solution;
3. disable non-required ports and services;
4. create a job aid for adding devices into the ESP;
5. update process documentation to include methodology for justification of ports and services;
6. define dynamic ports and services process;
7. enhance the change control process and issue documentation updates; and
8. perform training for applicable personnel.

CIP-007-1 R3 (RFC2013011943)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to Reliability*First*. URE submitted a revised Mitigation. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008837-2 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a comprehensive list of all applications, network devices, and operating systems in use within the ESP;
2. develop a process for managing multiple vendor updates, within the specified periodicity, including controls to ensure that URE receives, documents, and tracks notifications;
3. update Cyber Assets with applicable patches; and
4. conduct training and implementation of the process for managing multiple vendor updates.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R4 (RFC2013011945)

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008883-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. evaluate third-party vendors' anti-virus and malware testing for quality of evidence and test environment representative of URE's environment;
2. document the rolling wave approach and provide detail on the devices in the first wave and subsequent waves;
3. revise URE's procedure for process documentation to incorporate a cross-department peer review of CIP procedures;
4. implement a service contract with the vendor to provide support for the voltage regulator devices;
5. implement the solution provided by the vendor; and
6. create a job aid for adding devices to the ESP.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*.

CIP-007-1 R5 (RFC2012011453)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008889-2 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE's Mitigation Plan requires URE to:

1. create and implement a process for managing a manual log;
2. update procedure controls to specific log requirements for shared administrator accounts;

3. review the change control process and identify specific measures for renaming of admin accounts prior to production implementation;
4. update process documentation to address measures for renaming of admin accounts prior to production implementation;
5. execute a service contract with its vendor;
6. implement the software solution provided by the vendor;
7. create a job aid for adding devices into the ESP;
8. perform an exhaustive discovery of all accounts and where they are used;
9. develop tools to automate discovery of local accounts;
10. rename or remove privileged accounts, where feasible;
11. identify and implement tools for managing and reporting access;
12. create a policy for managing and reporting access to accounts that cannot be renamed; and
13. update governing procedure with detailed methods, process flows, and question and answer checklists.

CIP-007-1 R6 (RFC2012011454)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008886-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE Mitigation Plan required URE to submit a TFE, which was approved by Reliability*First*.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to Reliability*First*. After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-1 R6 (RFC2013013118)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT010169 and was submitted as non-public information to FERC in accordance with FERC orders. URE requested a Mitigation Plan completion date extension, which was granted by Reliability*First*.

URE's Mitigation Plan requires URE to:

1. verify that all network devices are communicating with URE's electronic security manager or submit a TFE;
2. develop and document a process to set and validate device and collector configurations for logging;
3. train applicable personnel on the process; and
4. submit a TFE.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[10]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on January 14, 2014. The NERC BOTCC approved the Settlement Agreement, including Reliability*First*'s assessment of a seventy-five thousand dollar ($75,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE violation history, which was considered an aggravating factor in penalty assessment;
2. URE self-reported most of the violations, as discussed above;
3. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;

[10] *See* 18 C.F.R. § 39.7(d)(4).

[11] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

4. URE had a compliance program at the time of the violation which Reliability*First* considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Reliability*First* determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE committed to performing above-and-beyond activities to implement reliability enhancements that exceed those actions that would achieve and maintain baseline compliance with the NERC CIP Reliability Standards and Requirements, as discussed above;
8. Reliability*First* considered that all the instant violations, as an aggregate, posed an elevated level of possible risk to URE's Cyber Assets, which was indicative of programmatic failure; and
9. Reliability*First* reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seventy-five thousand dollars ($75,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between Reliability*First* and URE, included as Attachment a;

b) Record documents for the violation of CIP-005-1 R2, included as Attachment b:
   1. URE's Self-Report;
   2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
   3. URE's Mitigation Plan designated as RFCMIT008835-2;
   4. URE's Certification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-005-3a R3, included as Attachment c:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as RFCMIT009920;

d) Record documents for the violation of CIP-005-3 R4 and CIP-007-3 R8, included as Attachment d:
   1. URE's Self-Report;
   2. URE's Self-Report;
   3. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form ;
   4. URE's Mitigation Plan to address CIP-005-3 R4 designated as RFCMIT008887-2;
   5. URE's Certification of Mitigation Plan Completion;
   6. Reliability*First*'s Verification of Mitigation Plan Completion;
   7. URE's Mitigation Plan to address CIP-0070-3 R8 designated as RFCMIT008888-1;
   8. URE's Certification of Mitigation Plan Completion;
   9. Reliability*First*'s Verification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-006-1 R1, included as Attachment e:
   1. URE's Self-Report;

2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT009390;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-006-1 R2, included as Attachment f:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT009265-1;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-007-1 R1, included as Attachment g:

1. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
2. URE's Mitigation Plan designated as RFCMIT009538;
3. URE's Certification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-007-1 R2, included as Attachment h:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
3. URE's Mitigation Plan designated as RFCMIT008836-3;

i) Record documents for the violation of CIP-007-1 R3, included as Attachment i:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
3. URE's Mitigation Plan designated as RFCMIT008837-2;
4. URE's Certification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-007-1 R4, included as Attachment j:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;

3. URE's Mitigation Plan designated as RFCMIT008883-1;
4. URE's Certification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-007-1 R5, included as Attachment k:

1. URE's Self-Report;
2. URE's Self-Report;
3. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form;
4. URE's Mitigation Plan designated as RFCMIT008889-2;

l) Record documents for the violation of CIP-007-1 R6 (RFC2012011454), included as Attachment l:

1. URE's Self-Report;
2. Reliability*First*'s Possible Violation (PV)/Find, Fix, and Track ("FFT") Identification Form ;
3. URE's Mitigation Plan designated as RFCMIT008886-2;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-007-1 R6 (RFC2013013118), included as Attachment m:

1. URE's Self-Report;
2. URE's Self-Report ; and
3. URE's Mitigation Plan designated as RFCMIT010169.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Director of Analytics & Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 - facsimile bob.wargo@rfirst.org Niki Schaefer* Managing Enforcement Attorney Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 - facsimile niki.schaefer@rfirst.org	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net L. Jason Blake* General Counsel Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (330) 456-2488 (330) 456-5408 – facsimile jason.blake@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Assistant General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
North American Electric Reliability Corporation
Senior Counsel and Associate Director, Enforcement Processing
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

February 27, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violation[3] of CIP-002-1. According to the Settlement Agreement, URE stipulates and agrees to the facts of the violation and has agreed to the assessed penalty of zero dollars ($0), in addition to other remedies and actions to mitigate the instant violation and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violation identified as NERC Violation Tracking Identification Number SPP201000414 is being filed in accordance with the NERC Rules of Procedure and the CMEP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 10, 2013, by and between SPP RE and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Southwest Power Pool Regional Entity	**Unidentified Registered Entity**	NOC-2259	SPP201000414	CIP-002-1	R2	High	$0

CIP-002-1

The purpose statement of Reliability Standard CIP-002-1 provides:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets. Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with

the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R2 provides: "Critical Asset Identification — The Responsible Entity[4] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary."

CIP-002-1 R2 has a "High" Violation Risk Factor (VRF) and a "Moderate" Violation Severity Level (VSL). The subject violation applies to URE's Transmission Operator (TOP) function.

During a Spot Check, SPP RE identified a violation of CIP-002 R2. Specifically, the SPP RE Audit Team concluded that the evaluation criteria utilized by URE in its risk-based assessment methodology (RBAM) to identify Critical Assets had not been properly applied. The URE RBAM consists of an engineering analysis, a consequence analysis, and a third-party analysis. The consequence analysis involves answering a set of questions for each asset evaluated. A different set of questions is provided for facilities in each of the following asset categories: generation, transmission, and control centers. SPP RE found that URE had improperly answered a consequence analysis question for its blackstart generator used for system restoration, and for its primary and backup control centers (PCC and BCC). As a result, URE failed to identify these assets as Critical Assets.

During a Compliance Audit SPP RE identified a violation of CIP-002-3 R2. SPP RE concluded that when URE applied its RBAM to identify its Critical Assets, URE did not correctly answer a risk assessment question for its PCC, BCC, and a substation. Consequently, URE failed to identify its PCC, BCC, and the substation as Critical Assets.

The instant violation is a consolidation of the two violations of CIP-002 R2 identified by SPP RE in the Spot Check (SPP201000414) and in the Compliance Audit (SPP2013012066). SPP RE issued a Notice of Alleged Violation and Proposed Penalty or Sanction (NAVAPS) for SPP201000414. SPP RE proposed a penalty of $7,200 for the violation. URE responded to the NAVAPS contesting the violation and the proposed penalty. SPP RE and URE were unable to resolve this compliance issue, and URE requested a hearing. Pursuant to a Joint Motion to Suspend the Procedural Schedule, the Hearing Officer issued

[4] Within the text of Standard CIP-002, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

an order staying the hearing, pending approval of a Settlement Agreement by the NERC Board of Trustees Compliance Committee (BOTCC) and FERC.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE as a "Table 2" entity, through the present.

SPP RE determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, by not identifying the PCC and BCC as Critical Assets, these facilities may not be afforded the protections of CIP-003 through CIP-009. Without these protections, the PCC and BCC could be destroyed, degraded, misused, or otherwise rendered unavailable due to a cyber attack. In addition, under the bright-line criteria in CIP-002-5, primary and backup transmission control centers are designated as "Medium" impact. The risk to the reliability of the BPS was mitigated by the following factors. Because there are no Critical Cyber Assets (CCAs) associated with URE's blackstart units, URE's failure to identify a blackstart unit as a Critical Asset is moot with regard to application of the protections provided by CIP-003 through CIP-009. Additionally, the blackstart unit and the affected substation are designated as "Low" impact under the bright-line criteria established in CIP-002-5. Accordingly, these facilities would not require the extensive protections provided by CIP-003-5 through CIP-009-5. SPP RE also considered URE's size and location as mitigating factors to the reliability of the BPS.

In addition, URE also had corporate physical and electronic cyber security measures in place. Its electric operations were separated via firewalls from other operations. There was physical security in place including a door access security system, card readers, and cameras that were continuously monitored. In addition, there were electronic security measures in place such as firewalls and intrusion detection systems for the Electronic Security Perimeter.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of zero dollars ($0) for the referenced violation. In reaching this determination, SPP RE considered the following factors:

1. the violation constituted URE's first occurrence of violation of the subject NERC Reliability Standard;
2. URE had a compliance program at the time of the violation, which SPP RE considered a mitigating factor;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

4. the violation did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
5. URE agreed to identify its control centers as Critical Assets and to bring any associated CCAs into compliance with CIP-003 through CIP-009; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of zero dollars ($0) is appropriate and bears a reasonable relation to the seriousness and duration of the violation.

Status of Mitigation Plan[5]

URE's Mitigation Plan to address its violation of CIP-002-1 R2 was submitted to SPP RE. URE submitted a revised Mitigation Plan. The Mitigation Plan was accepted by SPP RE on November 21, 2013 and approved by NERC on December 6, 2013. The Mitigation Plan for this violation is designated as SPPMIT004918-1 and was submitted as non-public information to FERC on December 6, 2013 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. adopt the CIP Standards Version 5 Bright-Line Criteria (V5 BLC) found in CIP-002- 5, Attachment 1 in lieu of maintaining a CIP Standards Version 3 compliant Risk Based Assessment Methodology;
2. identify Alternative Approach 2 in the NERC Cyber Security Standards Guidance (Revised) published September 5, 2013, for use in identifying Critical Assets;
3. identify its PCC and BCC, which meet one or more of the "High" or "Medium" V5 BLC, as its only Critical Assets;
4. identify as CCAs the Cyber Assets essential to the operation of any identified Critical Asset and meeting the qualifying criteria of CIP-002-3 Requirements R3.1, R3.2, or R3.3; and
5. apply the controls in CIP-003-3 through CIP-009-3 to those identified CCAs and any additional Cyber Assets brought into scope by the application of the requirements of CIP-003-3 through CIP-009-3.

[5] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 4, 2014. The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of a zero dollars ($0) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirement of the Commission-approved Reliability Standard and the underlying facts and circumstances of the violation at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. the violation constituted URE's first occurrence of violation of the subject NERC Reliability Standard;
2. URE had a compliance program at the time of the violation which SPP RE considered a mitigating factor, as discussed above;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. SPP RE determined that the violation did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
5. URE agreed to identify its control centers as Critical Assets and to bring any associated CCAs into compliance, as discussed above; and
6. SPP RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of zero dollars ($0) is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

---

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities, and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between SPP RE and URE, included as Attachment a;

b) SPP RE's Spot Check document, included as Attachment b;

c) URE's Compliance Audit document, included as Attachment c;

d) URE's Mitigation Plan designated as SPPMIT004918-1, included as Attachment d;

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Mr. Ron Ciesiel – General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, Arkansas 72223-4936 rciesiel.re@spp.org Office: 501-614-3265 Fax: 501-482-2025 Mr. Joe Gertsch - Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, Arkansas 72223-4936 Jgertsch.re@spp.org Office: 501-688-1672 Fax: 501-482-2025	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Mr. Jim Julian - Counsel to the SPP RE Chisenhall, Nestrud & Julian, P.A. Regions Center 400 West Capitol, Suite 2840 Little Rock, Arkansas 72201 jjulian@cnjlaw.com Office: 501-372-5800 Fax: 501-372-4941

Ms. Stephanie Kimp – Law Clerk Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, Arkansas 72223-4936 skimp.re@spp.org spprefileclerk@spp.org (Document Filing) Office: 501-688-8209 Mobile: 501-413-0683 Fax: 501-482-2025	*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVLIEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

March 31, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity (URE)
FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE) , NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of CIP-002-2 R3; CIP-005-3 R1 and R5; CIP-006-1 R1, R2 and R3; and CIP-007-1 R1 and R2. According to the Settlement Agreement, URE agreed and stipulated to the terms of the Settlement Agreement, and has agreed to the assessed penalty of four hundred sixty-five thousand dollars ($465,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC2012011042, WECC2012011043, WECC2012011044,

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

WECC2012011140, WECC2012011053, WECC2012011054, WECC2012011058 and WECC2012011059 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on September 19, 2013, by and between WECC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	URE	NOC-2205	WECC2012011042	CIP-002-2	R3	High	$465,000
			WECC2012011043	CIP-005-3	R1	Medium	
			WECC2012011044	CIP-005-3	R5	Lower	
			WECC2012011140	CIP-006-1	R1	Medium	
			WECC2012011053	CIP-006-1	R2	Medium	
			WECC2012011054	CIP-006-1	R3	Medium	
			WECC2012011058	CIP-007-1	R1	Medium	
			WECC2012011059	CIP-007-1	R2	Medium	

CIP-002-2 R3

The purpose statement of Reliability Standard CIP-002-2 provides:

NERC Standards CIP-002-2 through CIP-009-2 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.

These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-2 R3 provides:

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-2, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

CIP-002-2 R3 has a “High” Violation Risk Factor (VRF) and a “High” Violation Severity Level (VSL).

WECC performed an on-site Compliance Audit (Audit) of URE. WECC's Audit Team reviewed URE's Risk Based Assessment Methodology (RBAM) and associated lists of Critical Assets and Critical Cyber Assets (CCAs). In addition, WECC's Audit Team conducted facility site tours to confirm specific listings of CCAs. During the site tours, WECC's Audit Team identified nine discrepancies on URE's CCA lists.

WECC reviewed the Audit findings and determined that URE was in violation of CIP-002-2 R3 for failing to update its CCA lists when changes to these assets occurred. Specifically, URE's lists represented an inaccurate depiction for nine CCAs that have been removed from service, have been misidentified, or have been identified incorrectly on the CCA list.

WECC determined the duration of the violation to be from the date the first CCA was removed from service, through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the risk to the BPS was moderate because URE's failure to update the list of CCAs, as necessary, rendered these devices vulnerable to cyber attacks or misuse. The assets were located across five substations and the discrepancies occurred because URE's asset strategists failed to follow URE's validation process when changes occurred. WECC determined that URE's failure to confirm that corrections to the list are made and actions are recorded within its equipment validations process represents weak asset management practices. The risk was mitigated by the fact that URE afforded a number of protective measures to the nine CCAs at issue. Specifically, all the devices were physically secure and located within a Physical Security Perimeter (PSP). Physical access to the devices was limited to individuals who had Personnel Risk Assessments (PRAs) and cyber security training. Finally, physical and electronic access was logged and monitored and unauthorized access attempts would have triggered alarming to notify URE staff.

CIP-005-3 R1.5 and R1.6

The purpose statement of Reliability Standard CIP-005-3 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-3 R1 has a "Medium" VRF and a "Severe" VSL.[4]

During URE's Audit, WECC's Audit Team reviewed URE's network diagrams, documentation of Critical and non-critical Cyber Assets within URE's Electronic Security Perimeters (ESPs), all electronic access points to the ESPs, and the Cyber Assets deployed for the access control and monitoring of these access points. In addition, the Audit Team conducted facility site tours to confirm specific listings of assets. During the site tours, the Audit Team identified several access control and monitoring assets that were not identified in URE's network diagrams. For approximately 60 assets URE did not classify the devices as access control and monitoring devices. URE only took into consideration access points and failed to consider assets that control or log access. Because URE failed to identify these assets as access control and monitoring assets, it did not afford the protective measures specified in CIP-005-3 R1.5 to these assets.

WECC reviewed the Audit findings and determined that URE failed to maintain documentation of all electronic access points to the ESPs and for 60 assets deployed for the access control and monitoring of these access points, in violation of CIP-005-3 R1.6. URE also failed to afford these unidentified access control and monitoring Cyber Assets 27 protective measures, as required by CIP-005-3 R1.5.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the present.

[4] WECC assessed the VRF and VSL for this violation at the requirement level.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was moderate because URE failed to afford 27 protections to 60 assets associated with access points and access control and monitoring within 100 percent of URE's ESPs. The risk was mitigated by the fact that the Cyber Assets physically reside within the PSP and ESP they were responsible for protecting. Therefore, the Cyber Assets were given physical and electronic monitoring and alarming protection at all time. In addition, URE has a system network that supports systems critical to URE and where traffic is segregated by firewalls. Furthermore, URE's physical access controls restrict access to only approved personnel with approved PRAs and cyber security training.

CIP-005-3 R5

CIP-005-3 R5 provides:

> R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.
>
> > R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
> >
> > R5.2. The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
> >
> > R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

CIP-005-3 R5 has a “Lower” VRF and a “Severe” VSL.

During URE's Audit, WECC’s Audit Team reviewed URE's network drawings and configuration manuals and conducted facility site tours to verify URE's assets in the network drawings. During the site tour, the Audit Team identified a discrepancy in a network drawing. Specifically, a network switch was identified on the drawing but was no longer located within the ESP. After discussing the discrepancy with URE, URE stated that the network switch was redeployed to a new ESP.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

WECC reviewed the Audit findings and determined that URE was in violation of CIP-005-3 R5.2 for failing to update its documentation to reflect the redeployed CCAs within 90 calendar days of the change.

WECC determined the violation began 90 days after URE failed to update its documentation, and continued through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to update the ESP network drawing when the asset was removed, the documentation was accurate for URE's remaining ESPs. In addition, all traffic to and from ESPs must pass through firewalls, which are configured to restrict, monitor, and alert upon suspected malicious activity. Further, URE's substation is surrounded by a six-foot-high chain link fence with three-strand barbed wire on top. URE restricts physical access to individuals with PRAs and cyber security training.

CIP-006-1 R1.2 and R1.8

The purpose statement of Reliability Standard CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009 . . . ."

CIP-006-1 R1 provides in pertinent part:

> The Responsible Entity shall comply with the following requirements of Standard CIP-006:
>
> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > ***
> >
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005

Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.[5]

During URE's Audit, WECC's Audit Team issued a data request to URE that specified 12 Critical Asset sites the Audit Team would visit. During the course of the site visits, the Audit Team reviewed URE's physical security of CCAs and determined URE failed to identify all access points through each PSP (R1.2) and failed to ensure devices used in the physical access control and monitoring of PSPs were protected per CIP-006-1 R1.8.

WECC's Audit Team identified seven instances at four PSPs where all access points to the PSPs were not documented, as follows:

1. URE failed to identify and document a physical access point through the PSP. The door was secured with a card reader, but had no monitoring measures in place and was not identified on the PSP drawings;

2. URE failed to identify an exit-only access point. The door was locked and secured from outside access by restricted key, and had door contacts that would issue an audible alarm if opened. Additionally, the door was monitored by a camera;

3. URE failed to identify four access points. Specifically, one physical access point (a door) on the first floor and three physical access points (two windows, one roof hatch) on the second floor were not identified. URE believed the door to be sealed, and as such not required to be identified as an access point; and

4. URE failed to identify a physical access point through a PSP. On the south end of the PSP, a roof hatch and two metal plates were installed. All three points of access (roof hatch, two metal plates) had contact alarms installed which would alert upon being opened. The roof hatch was locked from the inside with a dead bolt. The three points of access, which were considered one access point (the equivalent of a double door having two points of access) were not identified or documented as access points to the PSP.

In addition, WECC's Audit Team determined URE was not classifying workstations and control panels capable of granting and revoking access to PSPs as devices used in the access control and monitoring of

[5] WECC assessed the VRF and VSL for this violation at the requirement level.

PSPs. Because URE did not identify these devices as physical access control and monitoring devices, URE could not ensure the devices were provided the protections of CIP-006-1 R1.8.

WECC determined that URE was in violation of CIP-006-1 R1.2 for failing to identify seven PSP access points, and for failing to ensure 118 Cyber Assets used in the access control and monitoring of PSPs were afforded the protections specified in CIP-006-1 R1.8.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE, through the date, when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk to the BPS was moderate because URE failed to afford 27 protections to 118 Cyber Assets, and failed to identify seven access points to four PSPs. However, the risk was mitigated by several factors. The Cyber Assets at issue physically reside within the PSP they were responsible for protecting and were afforded physical and electronic monitoring and alarming at all times. In addition, URE implemented a monitoring solution that would alert URE's personnel if an access point were opened. Furthermore, URE implemented a physical access control that restricts access to personnel with PRAs and cyber security training.

CIP-006-1 R2

CIP-006-1 R2 provides:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> > R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

> R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" VRF and a "Severe" VSL.

During URE's Audit, WECC's Audit Team identified one access point (two metal plates) next to a fire escape hatch in the ceiling that was not locked. The two metal plates had contact alarms which would alert upon being opened; however, no operational or procedural controls to manage the physical access were implemented. Further, WECC's Audit Team issued a data request to URE, asking URE to describe what physical access protections were applied to the metal coverings. In response, URE confirmed that the two metal coverings, if removed, would generate an alarm. However, there were no additional operational or procedural controls installed to manage physical access.

WECC determined that URE was in violation of CIP-006-1 R2 for failing to document and implement operational and procedural controls to manage physical access at one access point to one substation at all times.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to afford operational controls to the access point, if the metal coverings were removed, an alarm would have sounded, alerting URE personnel of the opening. Also, URE's substation at issue was surrounded by a six-foot-high chain link fence with three-strand barbed wire on top. The fence has an intrusion detection system mounted throughout. URE restricted physical access to individuals with PRAs and cyber security training.

CIP-006-1 R3

CIP-006-1 R3 provides:

> R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

CIP-006-1 R3 has a "Medium" VRF and a "Severe" VSL.

During URE's Audit, WECC's Audit Team toured one of URE's substations. During the tour, the Audit Team discovered one access point (a door) located on the northwest side of the substation that was not identified on the PSP map provided by URE. The door had no exterior hardware providing for ingress to the PSP and had no means of monitoring in the event the door was open (forced or propped). WECC's Audit Team also toured URE's another transmission operator control PSP. During this site tour, the auditors discovered three access points (doors) which did not have door contacts installed. Therefore, the access points could not be monitored for door-forced-open or door-held-open events.

WECC determined that URE was in violation of CIP-006-1 R3 for failing to implement technical controls for monitoring physical access at all times at four access points (doors) to two PSPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed to monitor physical access at four access points to two PSPs for approximately four years. Because URE failed to implement these controls, URE could not determine if one of the unmonitored access points were left propped open, thereby allowing unauthorized access to the 72 CCAs located in one PSP and 31 CCAs located at another PSP. However, the risk was mitigated by several factors. The access point at issue was egress only with no external hardware. Also, the substation was surrounded by a six-foot-high, chain link fence with three-strand barbed wire on top and an intrusion detection system mounted throughout. The fence restricted physical access to individuals with PRAs and cyber security training. The other PSP access points had ingress card readers installed, which had to be used to gain access to the locked doors. URE employs security guards, stationed on the ground floor, who verify all personnel that enters the building and validate personnel's access cards.

CIP-007-1 R1

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009 . . . ."

CIP-007-1 R1 provides:

> The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):
>
> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> R1.1. The Responsible Entity shall create, implement, and maintain cybersecurity test procedures in a manner that minimizes adverse effects on the production system or its operation.
>
> R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
>
> R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

During URE's Audit, WECC's Audit Team determined URE was not able to produce records of testing for all significant changes to Cyber Assets within an ESP. Specifically, URE could not produce records for three significant changes made to an asset area and four significant changes made to another asset area. In addition, the Audit Team confirmed that URE only performs functional testing and does not perform security testing as part of its test procedures.

WECC determined that URE did not provide any evidence of security testing performance for seven significant changes made to Cyber Assets in the two asset area ESPs. Because URE did not perform

security testing on these seven assets, URE could not ensure that these changes did not adversely affect existing cyber security controls.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed to perform security testing on seven assets and could not ensure systems were secure prior to the implementation of software upgrades, vendor releases, version upgrades, and system upgrades. However, the risk was mitigated by several factors. URE had layers of security controls in place during the pendency of the violation. Specifically, URE had network separation with firewall technology, host intrusion detection systems, annual cyber vulnerability assessments, and monitoring and alerting processes that included third-party analysis and reporting. Additionally, all traffic to and from URE's ESPs passed through multiple firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Lastly, URE performs functionality testing on all assets prior to making significant changes. This type of testing verifies that the device operates correctly prior to being released into production.

CIP-007-1 R2

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
> >
> > R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a “Medium” VRF and a “Severe” VSL.

During URE's Audit, WECC's Audit Team identified eight power supply controllers that had ports open and were not required for normal or emergency operations, but could not be disabled. The ports were used for remote logging and for securing systems determined to be CCAs.

WECC determined URE was in violation of CIP-007-1 R2 for failing to enable only those ports and services required for normal and emergency operations. WECC also determined that URE failed to document compensating controls and submit a Technical Feasibility Exception (TFE) for the eight devices that had ports open that were not required but could not be disabled.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed to document compensating controls and submit a TFE for the eight RAS devices that have ports open that are not required but could not be disabled. The ports were used for remote logging and for securing systems determined to be CCAs. However, the risk was mitigated by several factors. URE used network and host intrusion detection and protection systems to provide protection against attacks, exploits, and vulnerabilities. This system included network separation and firewall technology which was monitored at all times. URE's devices were physically secure because URE used ID badge systems, cameras, and physical security monitors to deter and prevent unauthorized physical access to areas or systems. Further, all individuals with access to ESPs and PSPs had PRAs and cyber security training.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of four hundred sixty-five thousand dollars ($465,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE's prior violation history for CIP-006-1 R1, which was not considered an aggravating factor in the penalty determination;[6]
2. URE's prior violation history for CIP-007-1 R2, which was considered an aggravating factor in the penalty determination;[7]

[6] Although this was URE's third violation of CIP-006-1 R1, WECC determined the first and second instances are distinct from this violation because they relate to separate sub-requirements. As a result, WECC determined that this was not recurring conduct and aggravation was not warranted for the violation addressed herein.

[7] This was URE's second violation of CIP-007-1 R2. Similar to the instant violation, the first violation involved URE's failure to establish and document a process to ensure that only those ports and services required for normal and emergency

3. URE's prior violation history for CIP-007-1 R1 was not considered as an aggravating factor by WECC;[8]
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of four hundred sixty-five thousand dollars ($465,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[9]

CIP-002-2 R3

URE's Mitigation Plan to address its violation of CIP-002-2 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. update its RBAM to clarify timelines and requirements;
2. develop a procedure for semi-annual sampling and verification of the CCA list;
3. create a process map for management of relevant changes that can be used by all stakeholders;
4. select a common database for CCAs;
5. establish and complete semi-annual CCA audit; and

operations were enabled for approximately 400 devices. Therefore, WECC considered the previous violation as an aggravating factor in the penalty determination.

[8] This was URE's fourth violation of CIP-007-1 R1. Because the prior violations were concurrent with the instant violation, WECC did not consider them as an aggravating factor in the penalty determination.

[9] *See* 18 C.F.R § 39.7(d)(7).

6. review the status of the audit and make appropriate updates.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3 R1

URE's Mitigation Plan to address its violation of CIP-005-3 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. perform a detailed analysis and extent of condition of the entire CIP-related environment to determine whether existing documentation needs to be updated or clarified, and whether additional systems or assets need to be included;
2. finalize the implementation plan to ensure ongoing compliance with CIP-005 R1;
3. create a detailed scope of work and project plan based on the completed extent of condition review;
4. create documentation and processes required to support completion of the project;
5. develop training materials needed to ensure all stakeholders are trained as required on the changes being implemented into the CIP environment;
6. complete implementation of the updated processes; and
7. complete training for all key stakeholders as required.

CIP-005-3 R5

URE's Mitigation Plan to address its violation of CIP-005-3 R5 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an extent of condition review to ensure URE fully understands the overall scope of the finding and include all relevant assets and areas in the remediation activities;
2. create a process and procedure for performing annual site visits and walk-downs of ESPs;
3. implement the site visit and walk-down procedure;
4. create a formalized, documented process that will ensure that drawings and associated documentation is consistently managed in compliance with the requirements of CIP-005 R5;

5. develop training related to the new process for key stakeholders; and
6. implement the new process and training.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. provide site contacts with special locks and instructions in order to control access at identified sites;
2. have the applicable stakeholders meet quarterly to review Critical Asset ESP and PSPs;
3. identify resources and draft a timeline to remove assets out of ESPs;
4. update the Cyber Asset list with additional fields and include a change tab to document all changes;
5. move the assets at issue out of the ESP;
6. document a communication process to notify key stakeholders when an asset is added to existing ESPs; and
7. update documentation to reflect change at the locations at issue.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R2

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review the CIP-006-3 R4 (CIP-006-1 R2) requirement regarding the definition of access point with the manager, supervisor, security vendor and physical security specialists;
2. instruct the security vendor to eliminate the roof hatch from being an access point;
3. reconfigure the PSP and install card readers and door contacts on the interior door that controls access to the PSP;

4. update the diagram for a substation when changes are made to the PSP; and
5. implement a quarterly PSP review process to review PSP diagrams for accuracy.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R3

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. hire additional resources to conduct PSP site visits and review diagrams for accuracy;
2. install the missing door contacts to two facilities, and update the diagrams;
3. implement quarterly PSP review processes which include reviewing physical access controls at PSPs; and
4. update PSP diagrams to a standard format.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an extent of condition review to identify the gaps in the process and establish what assets areas are impacted;
2. create a plan (scope of work) with additional, specific milestones and identify key stakeholders and roles and responsibilities associated with the work to be completed. The plan includes standardized test criteria and test plans, cyber security controls checklist, quality assurance processes, and description of maintaining and storing evidence. The plan also includes integration into existing change management procedures, as appropriate;
3. create a training plan to be delivered to key stakeholders involved in the security controls testing process;
4. complete implementation of the modified test procedures;
5. update documentation and associated information as appropriate;

6. complete training of key stakeholders; and
7. implement effective controls to ensure ongoing compliance.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete a targeted port scan of the power supply controllers to determine a complete list of all of the open ports;
2. review all vendor ports and services documentation;
3. update the list to reflect ports and submit a TFE;
4. perform an extent of condition review to ensure the overall scope is clearly defined and understood;
5. evaluate the other devices to confirm the accuracy of the list, and determine whether any additional TFEs are required; and
8. update URE's list and complete and submit TFEs if required.

URE certified on that the above Mitigation Plan requirements were completed. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[10]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[11] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 5,

[10] *See* 18 C.F.R. § 39.7(d)(4).
[11] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a four hundred sixty-five thousand dollar ($465,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE's prior violations for CIP-006-1 R1, CIP-007-1 R1 and R2, as discussed above;
2. URE had a compliance program at the time of the violations which WECC considered a mitigating factor, as discussed above;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
6. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of four hundred sixty-five thousand dollars ($465,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Mark Maher*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(360) 713-9598
(801) 582-3918 – facsimile
Mark@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

Sonia C. Mendonça*
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

Chris Luras*
Director of Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: URE
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity (URE), FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of CIP-005-1 R1, CIP-005-3 R4, CIP-007-1 R1, R3, and R6, CIP-007-2a R4, and CIP-007-3a R2, R5, and R8. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty-five thousand dollars ($155,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC2012010739, WECC2012010740, WECC2012011029, WECC2012010439, WECC2012011031, WECC2012011329, WECC2012011032, WECC2012011034, and WECC2012010741 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-2284	WECC2012010739	CIP-005-1	R1; R1.1; R1.5; R1.6	Medium	$155,000
			WECC2012010740	CIP-005-3	R4	Medium	
			WECC2012011029	CIP-007-1	R1	Medium	
			WECC2012010439	CIP-007-3a	R2	Medium	
			WECC2012011031	CIP-007-1	R3	Lower	
			WECC2012011329	CIP-007-2a	R4	Medium	
			WECC2012011032	CIP-007-3a	R5; R5.2.3; R5.3.3	Medium	
			WECC2012011034	CIP-007-1	R6	Lower	
			WECC2012010741	CIP-007-3a	R8	Medium	

WECC performed a Compliance Audit of URE (Compliance Audit). During the course of the Compliance Audit, WECC's Audit Team reviewed a series of Self-Reports pertaining to violations of the CIP Reliability Standards that were submitted by URE in the months leading up to the Compliance Audit.

CIP-005-1 R1 (WECC2012010739)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity[4] shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
>
> ***
>
> R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
>
> R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical

[4] Within the text of the CIP Standards included in this Notice of Penalty, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-1 R1 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).[5]

URE submitted a Self-Report stating that it failed to ensure that Cyber Assets used in the electronic access control and monitoring of the Electronic Security Perimeters (ESPs) were afforded the protective measures specified in CIP-005-1 R1.5. WECC determined that URE did not document ports required for normal and emergency operations for 12 Cyber Assets consisting of routers and firewalls. As a result, URE could not ensure that only the ports and services required for normal and emergency operations were enabled on these Cyber Assets as required by CIP-005 R2.

In addition, during the Compliance Audit, WECC determined that URE failed to identify 24 access points to the ESP as required by CIP-005-1 R1.1. Further, WECC determined that URE failed to identify 29 Cyber Assets used in the access control and monitoring of access points, a violation of CIP-005-1 R1.6. The 29 Cyber Assets consisted of servers and appliance devices.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to identify 24 access points to the ESP (R1.1), for failing to ensure 12 Cyber Assets used in the access control and monitoring of the ESPs were afforded the protections of CIP-005 R2.2 (R1.5), and for failing to identify 29 Cyber Assets used in the access control and monitoring of access points (R1.6). All of URE's ESPs were affected.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until mitigated.

WECC determined that this violation poses a moderate risk to the reliability of the bulk power system (BPS), but does not pose a serious or substantial risk. Specifically, URE's failure to identify and afford protections to 65 Cyber Assets located within URE's ESPs rendered those devices vulnerable to exploitation. However, each of the ESPs is equipped with intrusion detection systems (IDS) and access point protections, including externally-connected communication end points. All traffic to and from the ESPs must first pass through firewalls, which are configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices reside within physically secure areas where

[5] WECC assessed the VSL for this violation at the sub-requirement level.

physical access is restricted to individuals with approved Personnel Risk Assessments (PRAs) and access is restricted through the use of key cards.

CIP-005-3 R4 (WECC2012010740)

The purpose statement of Reliability Standard CIP-005-3 provides in pertinent part: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-3 R4 provides:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings;
>
> R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-3 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during URE's an annual internal documentation sufficiency review, URE discovered it did not have certain evidence associated with its cyber vulnerability

assessment (CVA) for the previous year. Specifically, URE could not provide documentation demonstrating that it conducted a CVA of 12 electronic access points during that year.

URE reported that insufficient coordination between URE's business teams resulted in URE's failure to perform a CVA on the 12 access points. The electronic access points consisted of routers and firewalls with electronic access to URE's ESPs. URE conducted a full CVA the following year for these access points.

WECC determined that URE had a violation of CIP-005-3 R4 for failing to perform a CVA of all electronic access points to the ESPs at least annually. WECC confirmed that URE's failure to perform a CVA was for the same devices at issue in the CIP-005-1 R1 violation described above (WECC2012010739).

WECC determined the duration of the violation to be for the calendar year that URE missed its CVA.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to perform a CVA on the 12 access points in question, it did perform a CVA on its other access points. In addition, the affected ESPs were equipped with IDS and access point protections including externally-connected communication end points. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices resided within physically-secure areas where physical access was restricted to individuals with approved PRAs, and access was restricted through use of key cards.

CIP-007-1 R1 (WECC2012011029)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-1 R1 provides:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and

version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had failed to maintain complete and accurate cyber security control test results for significant changes on Cyber Assets. Specifically, URE reported that after it installed log data collection software, it performed testing on a "non-statistical, judgmental sample of devices." However, it did not perform testing on all covered devices where the software was installed.

During the Compliance Audit, WECC reviewed URE's cyber security test procedures and determined that URE performs cyber security control tests prior to the implementation of new Cyber Assets and when significant changes to existing Cyber Assets occur. However, WECC determined that for 40 Cyber Assets located within two ESPs, URE did not perform complete cyber security control testing after installing the software on those devices. The devices consisted of 27 CCAs and 13 non-critical Cyber Assets.

WECC determined that URE had a violation of CIP-007-1 R1 for failing to ensure all Cyber Assets have complete cyber security control testing and results for all significant changes to Cyber Assets within the ESPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that 40 Cyber Assets within two

ESPs were secure following the significant change rendered those devices vulnerable to potential exploitation, potentially allowing unauthorized access to the ESPs. However, URE's networks were isolated from its corporate environment and its internet, and all traffic to and from the ESPs must have first passed through firewalls (which were configured to restrict, monitor, and alert upon suspected malicious activity or traffic). Also, the affected devices resided within physically-secure areas where physical access was restricted to approved, trained, and vetted individuals and access was restricted and monitored through the use of key cards.

CIP-007-3a R2 (WECC2012010439)

The purpose statement of Reliability Standard CIP-007-3a provides in pertinent part: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-3a R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
>
> R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

CIP-007-3a R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during an annual internal documentation sufficiency review, it discovered that the CVA evidence associated with certain ESPs was deficient. Specifically, URE did

not document ports required for normal and emergency operations for 18 devices. As such, for 9 Critical Cyber Assets (CCAs) and 9 non-critical Cyber Assets, URE could not ensure that only those ports required for normal and emergency operations were enabled.

Subsequently, URE submitted a second Self-Report reporting an increase in the scope of the noncompliance. Specifically, URE found that its CVA did not distinguish ports and services required for normal and emergency operations from all other ports and services. The URE baseline documents for over 500 devices (including approximately 400 CCAs and over 100 non-critical Cyber Assets) did not indicate whether ports and services were required for normal or emergency operations. Because of this failure, URE could not ensure only those ports and services required for normal and emergency operations were enabled.

WECC determined that URE had a violation of CIP-007-3a R2 for failing to enable only those ports and services required for normal and emergency operations. WECC further determined that URE failed to establish a process to ensure that only those ports and services required for normal and emergency operations are enabled. WECC determined that the violation affected over 500 devices used to support all of URE's ESPs.

WECC determined the duration of the violation to be from when URE failed to maintain proper documentation of ports and services through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that only those ports and services required for normal and emergency operations rendered over 500 devices (and their associated ESPs) vulnerable to potential exploitation, because URE could not ensure that only required ports and services were enabled. However, URE used signature-based filtered IDS to provide protection against attacks, exploits, vulnerabilities, and policy violations. URE's IDS was managed, and the network systems were monitored and activity logged at all times. URE represented that its devices were physically secure, and that it used physical security monitors, identification (ID) badge systems, cameras, guards, and other prevention measures to deter or prevent unauthorized access to its network systems. Further, all individuals with access to URE's ESPs and Physical Security Perimeters (PSPs) had PRAs and proper training.

CIP-007-1 R3 (WECC2012011031)

CIP-007-1 R3 provides:

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during its pre-audit data request response process, it discovered that it did not have a log or other tracking mechanism for all security patches or all Cyber Assets released during the audit period. Consequently, URE could not establish that it had documented its evaluation of all applicable security patches within 30 calendar days of their availability.

During the Compliance Audit, WECC reviewed URE's Self-Report. WECC determined that while URE used a third-party contractor to perform some security patch management services, a number of Cyber Assets were not covered by this patching program. As a result, URE could not establish that it had documented its evaluation of all applicable security patches within 30 days of availability for nearly 500 Cyber Assets within two ESPs. The devices consisted of approximately 20 CCAs and over 450 non-critical Cyber Assets.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that all Cyber Assets within the ESPs had an established, documented, and implemented security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches put these devices at risk of being compromised by known vulnerabilities. WECC considered that a large number of devices were affected and an unknown number of patches were missed (i.e., each device may have missed multiple patches). However, the affected devices resided within physically-secure areas where physical access was restricted to approved and trained individuals, and where physical access was restricted and monitored through the use of key cards. URE's networks were isolated from its corporate environment and from the internet. Traffic to and from the ESPs must have first passed through firewalls. URE installed anti-virus prevention tools on the affected devices, and the devices were monitored by IDS. In addition, URE filed a Technical Feasibility Exception (TFE) for nearly 80% of these devices, indicating that the manufacturer does not provide patches.

CIP-007-2a R4 (WECC2012011329)

The purpose statement of Reliability Standard CIP-007-2a provides: "Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-2a R4 provides:

> R4. Malicious Software Prevention —The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-2a R4 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC discovered that URE failed to use anti-virus software and other malicious software prevention tools, where technically feasible, on three Cyber Assets located within two ESPs. Specifically, WECC discovered that one network scanner and two application whitelisting devices did not have anti-virus or malware tools installed when commissioned. The network scanner logged vulnerabilities on the control systems to patch management, and the whitelisting devices prevented the execution of unauthorized code. URE later submitted a TFE, indicating that it was not technically feasible to install anti-virus protection on the two whitelisting devices.

WECC determined that URE had a violation of CIP-007-2a R4 for failing to use anti-virus software and other prevention tools on the network scanner Cyber Asset where prevention tools were technically feasible to install. The network scanner Cyber Asset resided within an ESP.

WECC determined the duration of the violation to be from the day the devices were commissioned through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The affected asset resided within a physically-secure area where physical access was restricted to approved and trained individuals. URE's networks were isolated from its corporate environment and from the internet. All traffic to and from the ESP must have first passed through firewalls. Further, URE installed anti-virus and other malicious software prevention tools on all other capable devices on the affected network, thus ensuring that any virus or malicious software would not go beyond the affected device (had the device been compromised).

CIP-007-3a R5 (WECC2012011032)

CIP-007-3a R5 provides in pertinent part:

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

***

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

CIP-007-3a R5 has a "Medium" VRF and a "Severe" VSL.[6]

URE submitted a Self-Report addressing noncompliance with CIP-007-1 R5. Specifically, URE stated that it failed to have a policy for managing the use of shared accounts that could generate an audit trail (R5.2.3).

[6] WECC assessed the VRF at the sub-requirement level.

During the Compliance Audit, WECC determined that for over 500 devices, URE failed to have a policy for managing the use of shared accounts that could generate an audit trail. URE stated that it had controls in place for managing who had access to shared accounts, but no process in place to determine who was using the shared account at any given time. Consequently, URE could not provide evidence of an audit trail of the account use (automated or manual) as required by R5.2.3. The devices included network devices, human machine interfaces, industrial controllers, and printers located in two ESPs.

URE submitted TFEs for this Standard, which WECC approved. As a result, the number of devices associated with this violation was reduced from over 500 to approximately 120 devices. Subsequently, URE submitted amendments to the approved TFEs addressing the feasibility of some of the devices addressed herein. At this time, WECC is reviewing the technical feasibility of URE's devices associated with the amended TFEs.

WECC also determined that URE failed to ensure passwords were changed on an annual basis (R5.3.3). During a CVA, URE identified 13 accounts (10 service accounts and 3 individual user accounts) whose passwords had not been changed in over a year.

WECC determined that URE had a violation of CIP-007-3a R5 for failing to create an audit trail of shared account use (R5.2.3), and for failing to ensure passwords are changed on at least an annual basis (R5.3.3).

WECC determined the duration of the violation to be from the date on which URE mitigated a prior violation of CIP-007-1 R5 through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE had controls in place for managing who has access to shared accounts, but it failed to establish the technical and procedural controls to manage shared accounts. As a result, URE could not know who was using the shared account at any given time. In addition, URE failed to ensure that passwords were changed on at least an annual basis. However, URE's networks were isolated from its corporate environment and from the internet. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the devices in scope resided within physically-secure areas where physical access was restricted to individuals with approved PRAs and training and where physical access was restricted and monitored through use of key cards. In addition, the devices were actively monitored by IDS.

CIP-007-1 R6 (WECC2012011034)
CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
>
> R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
>
> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that some of its devices were not sending system event logs to URE's centralized logging server, the Security Information and Event Management (SIEM) system. During the Compliance Audit, WECC determined that over 500 devices were affected, consisting of nearly 400 CCAs and over 100 Cyber Assets. The devices included network devices, human machine interfaces, industrial controllers, and printers. The devices were located within two ESPs.

URE stated it had failed to submit TFEs for a large number of devices where it was technically infeasible for the device to implement automated tools to monitor system events that are related to cyber security. Specifically, URE reported that it was technically infeasible to log or monitor system events on over 400 devices. URE reported that over 60 devices were technically capable of logging and monitoring, but were not properly configured to do so.

WECC determined that URE had a violation of CIP-007-1 R6 for failing to ensure that over 500 Cyber Assets within two ESPs were monitoring system events related to cyber security.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement logging and monitoring controls on all of its Cyber Assets could have allowed unauthorized access to those devices to go unnoticed and unchecked, potentially allowing for malicious access. However, the two affected ESPs were equipped with IDS and access point protections including externally connected communication end points. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices resided within physically-secure areas where access was restricted to individuals with approved PRAs and training; physical access to these areas was restricted and monitored through use of key cards. Lastly, although URE failed to implement controls on the affected Cyber Assets, URE implemented automated tools and organizational process controls to monitor system events on other Cyber Assets.

CIP-007-3a R8 (WECC2012010741)

CIP-007-3a R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-3a R8 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during an annual internal documentation sufficiency review, URE discovered that certain evidence associated with its vulnerability assessments was insufficient. Specifically, URE could not identify a formal document that clearly demonstrated that a CVA was performed in the prior calendar year. Consequently, URE did not have documentation of an action plan to remediate or mitigate any vulnerability identified in an assessment.

URE stated it had failed to perform a CVA on 18 devices. Of the 18 devices in scope, 9 devices were CCAs and 9 were non-critical Cyber Assets. The devices resided in URE's ESPs. The devices consisted of routers and switches used to support the networking functions of the ESPs. According to URE, insufficient coordination between its business teams resulted in URE's failure to perform a CVA on certain assets. URE conducted a full CVA in the following year that addressed the CIP-007 R8 requirements.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to perform a CVA of all Cyber Assets within an ESP at least annually. URE's failure to perform its CVA was for the same devices in scope of the CIP-007-3a R2 violation (WECC2012010439) described above.

WECC determined the duration of the violation to be for the calendar year for which the CVA was not performed on the 18 devices.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed a CVA on the remaining Cyber Assets. In addition, the ESPs affected by the violation were equipped with IDS and access point protections, including externally connected communication end points. All traffic to and from the ESPs must have first passed through

firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the 18 affected devices resided within physically-secure areas where physical access was restricted to individuals with approved PRAs and training; physical access was restricted and monitored through use of key cards.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty-five thousand dollars ($155,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC determined that URE's violation history warranted an aggravation of the monetary penalty;
2. URE self-reported the violations of CIP-005-1 R1 (WECC2012010739), CIP-005-3 R4 (WECC2012010740), and CIP-007-3a R8 (WECC2012010741);[7]
3. upon undertaking the actions outlined in its Mitigation Plans, URE took voluntary corrective action to remediate the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation, which WECC considered a mitigating factor;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. there was no evidence that the violations were intentional;
8. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred fifty-five thousand dollars ($155,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[7] WECC did not award self-reporting credit for the remaining self-reported violations as the Self-Reports were submitted in the months leading up to the Compliance Audit.

Status of Mitigation Plans[8]

CIP-005-1 R1 (WECC2012010739)
URE's Mitigation Plan to address its violation of CIP-005-1 R1 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. complete the implementation of new SIEM systems;
2. complete the implementation of new authentication, authorization, and accounting systems;
3. complete compliance activities for a jump server, existing secure sockets layer virtual private network systems, remote server adapter servers, and intelligent process solutions assets;
4. complete implementation of new log collection devices; and
5. complete compliance activities for active directory and energy management system upgrade.

CIP 005-3 R4 (WECC2012010740)
URE's Mitigation Plan to address its violation of CIP-005-3 R4 was accepted by WECC approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review and update its vulnerability assessment procedure;
2. establish a detailed workbook containing network statistics configuration dates for each affected CIP Cyber Asset;
3. create action plans to identify and document the results of all issues from the following year's CVA and track remediation or mitigation of vulnerabilities;
4. create a summary report for the CVA for the affected CIP Cyber Assets; and
5. conduct a review of overall controls, ports and services, and assessment results with key business and information security personnel.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

[8] *See* 18 C.F.R § 39.7(d)(6).

CIP-007-1 R1 (WECC2012011029)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. clarify its testing procedures to require better documentation;
2. initiate a periodic review of proposed changes and verification of completed significant changes to testing documents; and
3. train employees on how and what to do when performing significant change testing.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R2 (WECC2012010439)

URE's Mitigation Plan to address its violation of CIP-007-3a R2 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review all CVA documentation containing analyses of compiled ports and services and identify those ports and services where the accompanying justifications were not documented;
2. disable listening ports and enabled services that are not required for normal and emergency operations for all Cyber Assets subject to the compliance program at the time the CVA was conducted for all Cyber Assets;
3. for all ports and services that must remain listening and enabled, ensure that justifications are provided for each;
4. review and update its relevant CVA procedure to ensure all requirements are met;
5. establish a detailed workbook containing network statistics configuration data for each affected Cyber Asset;
6. create action plans to identify and document the results of all issues from the vulnerability assessment and track remediation or mitigation of vulnerabilities; and

7. conduct a review of overall controls, ports, services, and assessment results with key business and information security personnel.

URE submitted a Certification of Mitigation Plan Completion. WECC is verifying that URE's Mitigation Plan was completed.

CIP-007-1 R3 (WECC2012011031)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. enhance its patch management program (which includes the review, identification, tracking, and remediation for security patches);
2. have the relevant staff meet to review, approve, and document the review of security patches on its patch review tracking log. The patches are identified as part of the asset and configuration baseline management for every system and the related software.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-2a R4 (WECC2012011329)

URE's Mitigation Plan to address its violation of CIP-007-2a R4 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install anti-virus software on the network scanner Cyber Asset;
2. work with its vendor to test the functionality of the anti-virus software; and
3. work with its vendor to validate the operation of the asset and the anti-virus software after installation of the software.

After WECC's review of URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R5 (WECC2012011032)

URE's Mitigation Plan to address its violation of CIP-007-3a R5 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change or disable all systems accounts passwords and, where applicable, file TFEs for accounts whose passwords could not be changed;
2. create an operators account to eliminate general use by operators of the administrative shared account; and
3. update existing policies and procedures to address specifically the use of existing physical door systems (i.e., badge card readers) and security cameras, as a means to provide an audit trail of the use of the shared accounts.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R6 (WECC2012011034)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify, test, configure, and validate a logging client, including performing testing of the logging client and performing logging against the requirements;
2. implement a process whereby URE generates a monthly log report for certain assets configured with the logging client which is reviewed to confirm that those assets are in fact logging; and
3. identify systems which required TFEs for technical and operational infeasibility and file the appropriate TFEs with WECC.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R8 (WECC2012010741)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review and update its relevant CVA procedure;
2. establish a detailed workbook containing network statistics configuration data for each affected CIP Cyber Asset;
3. create an action plan to identify and document the results of all issues from vulnerability assessments and track remediation and mitigation of vulnerabilities;
4. create a summary report of its CVA for affected Cyber Assets; and
5. conduct a review of overall controls, ports and services, and assessment results.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2014. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifty-five thousand dollar ($155,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE's violation history, which WECC considered an aggravating factor, as described above;

[9] *See* 18 C.F.R. § 39.7(d)(4).

[10] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

2. URE self-reported the violations of CIP-005-1 R1 (WECC2012010739), CIP-005-3 R4 (WECC2012010740), and CIP-007-3a R8 (WECC2012010741), which WECC considered a mitigating factor, as described above;
3. upon undertaking the actions outlined in its Mitigation Plans, URE took voluntary corrective action to remediate the violations, which WECC considered a mitigating factor, as described above;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation, which WECC considered a mitigating factor, as discussed above;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. there was no evidence that the violations were intentional;
8. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty-five thousand dollars ($155,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REMOVED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Jim Robb*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6853
jrobb@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200

Sonia C. Mendonça*
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

Chris Luras*
Director of Compliance Risk Analysis & Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and

Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 29, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity (URE), FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because, based on information from Western Electricity Coordinating Council (WECC), URE does not dispute the violations[3] of CIP-007-1 R5 and R6 and the proposed ninety-eight thousand five-hundred dollar ($98,500) penalty to be assessed to URE. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

WECC2013012597 and WECC2013012598 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Notice of Confirmed Violation (NOCV) issued by WECC. The details of the findings and basis for the penalty are set forth in the NOCV and herein. This Notice of Penalty filing contains the basis for approval of the NOCV by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-2292	WECC2013012597	CIP-007-1	R5; R5.1.2	Lower	$98,500
			WECC2013012598	CIP-007-1	R6	Medium	

CIP-007-1 R5 (R5.1.2)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

***

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

***

CIP-007-1 R5 has a "Lower" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report stating that it was in violation of CIP-007 R5. Specifically, for over 30 workstations, URE failed to establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.

URE reported that it discovered the violation during a review of its CIP compliance program. During this review, it performed site visits to confirm that its asset lists and drawings were up to date. The workstations affected by the violation were used in the normal operation and maintenance of URE's Supervisory Control and Data Acquisition (SCADA) system, energy management system (EMS), and Remedial Action Scheme (RAS) system.

URE determined that the violation was a result of a server not being configured properly to receive logs of sufficient detail from the workstations at issue. Because URE failed to ensure the appropriate technical and procedural controls were established to generate logs of sufficient detail on these workstations, URE failed to create a historical audit trail of individual user access for a minimum of 90 days.

WECC determined that URE had a violation of CIP-007-1 R5 (R5.1.2) for failing to ensure that the workstations were generating logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, URE's failure to create historical audit trails of individual user account access could have aided in losing visibility to the affected workstations. Without logging procedures and controls, URE would not have been able to identify or receive alerts for forced attacks, multiple bad password attempts, or irregular logons to these workstations. If any of these events were not noticed or investigated, an unauthorized person could have gained access to URE's SCADA, EMS, or RAS systems.

However, the SCADA, EMS, and RAS systems were protected from unauthorized access by URE's authentication systems, which required a token and password before allowing log-in and access. In addition, URE had personnel responsible for monitoring network activity in real time. These personnel were trained to recognize and respond to anomalous events. In order to access the devices affected by the violation, personnel must have been on-site. The Physical Security Perimeters (PSPs) in which the affected devices were located only allowed access to authorized personnel. Further, URE's Physical Access Control System (PACS) would have discovered unauthorized access to the PSPs.

No unauthorized access is known to have occurred.

CIP-007-1 R6

CIP-007-1 R6 provides in pertinent part:

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R6. Specifically, URE failed to implement automated tools or organizational process controls to monitor system events related to cyber security for the same workstations described in the violation of CIP-007-1 R5 above. URE determined that the violation was a result of a server not being configured properly to receive logs of system events related to cyber security from the workstations.

Following the Self-Report, URE conducted an expanded extent-of-condition review. Following this review, URE discovered that approximately 150 servers and workstations and approximately 50 network switches were not forwarding logs to the log monitoring servers.

Because URE failed to ensure that the workstations had automated tools or organizational process controls to monitor system events, URE did not maintain logs of system events related to cyber security (R6.3) and did not retain such logs for 90 days (R6.4).

WECC determined that URE had a violation of CIP-007-1 R6 for failing to implement automated tools or organizational process controls to monitor system events that are related to cyber security.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until mitigated.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement automated tools or organizational process controls to monitor system events related to cyber security could have aided in potentially losing visibility to the workstations. Without logging procedures and controls, URE would not have been able to identify or receive alerts for forced attacks, multiple bad password attempts, or

irregular logons to workstations. If any of these events were not noticed or investigated, an unauthorized person could have gained access to URE's SCADA, EMS, or RAS systems.

However, the SCADA, EMS, and RAS systems were protected from unauthorized access by URE's authentication systems, which required a token and password before allowing log-in and access. In addition, URE had personnel responsible for monitoring network activity in real time. These personnel were trained to recognize and respond to anomalous events. In order to access the devices affected by the violation, personnel must have been on-site. Further, the PSPs in which the affected devices were located only allowed access to authorized personnel; URE's PACS would have discovered unauthorized access to the PSPs.

No unauthorized access is known to have occurred.

Regional Entity's Basis for Penalty

WECC assessed a penalty of ninety-eight thousand five hundred dollars ($98,500) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC determined that URE's compliance history warranted an aggravation of the monetary penalty;
2. URE self-reported the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of ninety-eight thousand five hundred dollars ($98,500) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[4]

CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to perform an extent-of-condition review, remediate the out-of-compliance state for the applicable systems, and verify that the systems were logging user account activity.

URE certified that the above Mitigation Plan requirements were completed. WECC is in the process of verifying the completion of URE's Mitigation Plan.

CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. address the non-compliant condition on the identified devices and systems;
2. assess options for how best to determine whether all CIP assets are consistently and effectively generating logs on an ongoing basis;
3. develop and implement a process for detecting and correcting situations where systems are not creating or forwarding logs;
4. identify and train personnel that will be responsible for utilizing the new process; and
5. complete and publish all documentation and procedures associated with the Mitigation Plan.

[4] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the NOCV and supporting documentation on May 5, 2014. The NERC BOTCC approved the NOCV, including WECC's assessment of a ninety-eight thousand five-hundred dollar ($98,500) financial penalty against URE based upon WECC's findings and determinations. In approving the NOCV, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. WECC determined that URE's compliance history warranted an aggravation of the monetary penalty, as discussed above;
2. URE self-reported the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the NOCV and believes that the assessed penalty of ninety-eight thousand five hundred dollars ($98,500) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Chris Luras* Director of Compliance Risk Analysis & Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 29, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] of CIP-002, CIP-004, CIP-005, CIP-006, and CIP-007. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC201000685, SERC201000568, SERC201000569, SERC2012010884, SERC201000729, SERC2012011010, SERC201000730, SERC2012011011, SERC201000682, SERC201000731, SERC2012010586, SERC2012010860, SERC2013012360, SERC201000679, SERC201000733, SERC2012010585, SERC201000683, SERC2012009109, SERC201000678, SERC201000734, SERC201000735, SERC2012010883, SERC201000566, SERC201000736, SERC201000570, SERC201000567, SERC2012011013 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on March 17, 2014, by and between SERC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC201000685	CIP-002-2	R2	High	$250,000
			SERC201000568	CIP-004-1	R3	Medium	
			SERC201000569	CIP-004-1	R4	Medium	
			SERC2012010884	CIP-004-3	R4	Lower	
			SERC201000729	CIP-005-1	R1:1.5	Medium	

[4] For consistency, this filing throughout uses the earliest enforceable version of the CIP Standard applicable to each violation.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC2012011010	CIP-005-1	R1	Medium	$250,000
			SERC201000730	CIP-005-1	R2:2.2	Medium	
			SERC2012011011	CIP-005-1	R3:3.2	Medium	
			SERC201000682	CIP-006-1	R1.1	Medium	
			SERC201000731	CIP-006-1	R1	Medium	
			SERC2012010586	CIP-006-1	R1	Medium	
			SERC2012010860	CIP-006-1	R1:1.8	Medium	
			SERC2013012360	CIP-006-3c	R1:1.6.1	Medium	
			SERC201000679	CIP-006-2	R3	Medium	
			SERC201000733	CIP-006-2	R3	Medium	
			SERC2012010585	CIP-006-1	R4	Medium	
			SERC201000683	CIP-006-3a	R4	Medium	
			SERC2012009109	CIP-006-3c	R6	Lower	
			SERC201000678	CIP-007-1	R1	Medium	
			SERC201000734	CIP-007-1	R2	Medium	
			SERC201000735	CIP-007-1	R3	Lower	
			SERC2012010883	CIP-007-3a	R3	Lower	
			SERC201000566	CIP-007-1	R4	Medium	

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC201000736	CIP-007-1	R4:4.2	Medium	$250,000
			SERC201000570	CIP-007-1	R5	Medium	
			SERC201000567	CIP-007-1	R6	Medium	
			SERC2012011013	CIP-007-3a	R8	Lower	

CIP-002-2

The purpose statement of Reliability Standard CIP-002-2 provides in pertinent part: "Standard CIP-002-2 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-2 R2 (SERC201000685)[5]

CIP-002-2 R2 provides: "Critical Asset Identification — The Responsible Entity[6] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary." [Footnote added.]

CIP-002-2 R2 has a "Medium" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL).

URE submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R2. Specifically, URE failed to update its Critical Asset list to reflect the commissioning of a substation identified as a Critical Asset.

[5] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

[6] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

URE commissioned a newly identified Critical Asset but did not add it to the Critical Asset list until approximately seven months later, the same date that URE conducted the annual review. At the time of the violation, the newly identified Critical Asset contained no Critical Cyber Assets (CCAs) and approximately 65 Cyber Assets. The root cause of the violation was URE's misinterpretation of the requirements of CIP-002 R2. At the time of the violation, URE interpreted and documented the Standard requirement language to require that it update its lists through the annual review for the following year.

SERC determined that URE was in violation of CIP-002-1 R2 because URE failed to update Critical Asset listings after a new Critical Asset was commissioned.

SERC determined the duration of the violation to be from the date the Critical Asset was commissioned through when the Critical Asset was added to URE's Critical Asset list.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE commissioned and secured the Critical Asset in accordance with the NERC Implementation Schedule for Critical Assets. URE did have and followed its documented risk-based assessment methodology. The Critical Asset did not contain any CCAs, thereby reducing the possibility of cyber compromise and limiting the number of NERC CIP Reliability Standard requirements applicable to it.

CIP-004

The purpose statement of Reliability Standard CIP-004 provides:

> Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1 R3 (SERC201000568)[7]

CIP-004-1 R3 provides in pertinent part:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> > R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
> >
> > R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
> >
> > R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that an employee was granted authorized unescorted physical access to a Physical Security Perimeter (PSP) without having a personnel risk assessment (PRA) performed.

URE granted authorized unescorted physical access to a single PSP to a single individual. URE removed this access approximately eight months later. URE stated that the individual had no need for physical access and did not enter or attempt to enter the PSP during this time. The individual completed the

[7] URE's violation applies from Version 1 through Version 2 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

annual URE CIP training approximately four months prior to being granted authorized unescorted physical access and did not have electronic access to CCAs. URE's processes and procedures related to physical and electronic access adequately addressed the requirements of CIP-004 R3. The violation involves 0.25% of the total individuals with access to PSPs.

SERC determined that URE was in violation of CIP-004-1 R3 because it failed to perform a PRA for one employee within 30 days of granting authorized unescorted physical access to CCAs.

SERC determined the duration of the violation to be from thirty days after physical access was granted through when access was revoked.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This individual did not have electronic access to CCAs. In addition, this individual was in good standing with URE and completed the annual URE CIP security training before receiving access. The individual never attempted to gain physical entrance into the PSP. The violation involved less than 1% of the total individuals with access to PSPs at the time of the violation.

CIP-004-1 R4 (SERC201000569)[8]

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
> >
> > R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

[8] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

CIP-004-1 R4 has a "Medium" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that a local account was not removed from two network devices within seven days as required by CIP-004-1 R4.

Specifically, a local user account with administrative privileges was not removed from two network devices for approximately 22 months after the individual associated with that account no longer required electronic access to CCAs. SERC determined that URE failed to maintain its access lists for personnel with authorized electronic access to CCAs.

While SERC was assessing the violation reported in the Self-Report, the SERC audit team discovered one additional instance of noncompliance, and URE self-reported one additional instance of noncompliance involving the same Standard and requirement. SERC treated these additional instances as an expansion of scope of the violation addressed herein. Following a Compliance Audit, a SERC audit team reported a violation of CIP-004-2 R4.1. URE failed to update its authorized unescorted physical access list within seven days as required. Specifically, one manager had unescorted physical access that was revoked, but URE failed to update its access list until approximately two months later. URE failed to maintain its access lists for personnel with authorized unescorted physical access to CCAs.

URE self-reported an additional noncompliance with CIP-004-3 R4. An individual with unescorted physical access to an identified PSP retired. URE personnel requested revocation of the individual's access on the next day, but failed to revoke unescorted physical access to the PSP until nine days after the request. URE failed to revoke access to CCAs within seven calendar days for personnel who no longer required such access.

SERC determined that URE was in violation of CIP-004-1 R4 for failing to remove unneeded access to CCAs within seven days and for failing to maintain access list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs.

SERC determined the duration of the violation for the first instance to be from when the Standard became mandatory and enforceable on URE through when access was removed from switches. SERC determined the duration of the violation for the second instance to be from seven days after access was removed through the date the access list was updated. SERC determined the duration of the violation for the third instance to be from seven days after the individual retired through the date the lists were updated.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Each of the personnel involved had the required CIP cyber security training and completed

PRAs. Each of the personnel involved were in good standing with the company, and none required access revocation because of a for-cause termination.

CIP-004-3 R4 (SERC2012010884)

CIP-004-3 R4 has a "Lower" VRF and a "Lower" VSL.

URE submitted a Self-Report to SERC stating that it granted two individuals access to a PSP without authorization from the designated authorizing officials pursuant to the established internal policy.

URE became aware of this occurrence while conducting a quarterly review. According to URE, the two individuals had access to the PSPs for approximately 55 days.

URE's internal policy requires authorized personnel to submit an online request and acquire approval by the designated officials for that PSP. Access managers are those who can authorize a request for unescorted access to a controlled URE facility. Access managers are typically plant managers, regional managers, or other responsible persons who assure only those individuals with an appropriate business need will be granted access.

URE did not submit an online request for approval for these two individuals, nor did the individuals receive permission by the authorized officials prior to receiving access. Due to the automated nature of the process, the failure to submit an online request resulted in the list of personnel with unescorted authorized cyber or authorized unescorted physical access to CCAs not being updated within the required period.

The two individuals who had access to the PSP without authorization from the access manager were the chief executive officer and a vice president. Both individuals had a completed PRA and otherwise met the requirements for CCA and PSP access.

SERC determined that URE had a violation of CIP-004-3 R4 for failing to follow its PSP access policy, which in turn resulted in a failure to maintain the list of personnel with authorized cyber, or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

SERC determined the duration of the violation to be from when access was granted to the two individuals without permission from the designated officials through when URE revoked access to the PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The two individuals at issue had received PRAs and cyber security training and had approved access to other PSPs. The violation was restricted to less than 1% of the individuals with PSP access at the time of the violation.

CIP-005-1

The purpose statement of Reliability Standard CIP-005 provides: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1: R1.5 (SERC201000729)[9]

CIP-005-1 R1 provides:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

[9] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-1 R1 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE. SERC included an audit detail letter in which SERC notified URE that CIP-005-1 R1 would be in scope during the scheduled Spot Check.

The Spot Check team reported that URE did not afford protective measures for assets used in the electronic access control and monitoring (EACM) of the Electronic Security Perimeters (ESPs), a violation of CIP-005-1 R1. Specifically, URE did not identify and protect all Cyber Assets deployed for the access control and monitoring of the ESPs.

During the Spot Check, SERC discovered that URE contracted with a managed security service provider (MSSP) to collect, identify, validate, and escalate events and monitor access points to URE's ESPs. In order to perform the contracted services, the MSSP located certain monitoring devices at URE's facilities. Those monitoring devices gathered information and sent it via secure channels to the MSSP's central servers, which were not located at URE's facilities. Because of this arrangement, the devices located at URE's facilities and the MSSP's central servers are EACM devices, and URE must afford them the protections listed in CIP-005-1 R1.5.

SERC analyzed the contract under which the MSSP performed services for URE and determined that the contract with the MSSP did not ensure that the MSSP's devices used in the access control and monitoring of URE's ESPs were afforded the protections listed in CIP-005-1 R1.5. In addition to URE's

failure to ensure contractually that the MSSP located the EACM devices within a PSP, URE also failed to provide evidence that it had provided the EACM devices with the required protections.

SERC determined that URE was in violation of CIP-005 R1.5 because it failed to provide evidence that it provided the required protective measures to Cyber Assets used in the access control and monitoring of the ESPs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through the present.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE allowed CCA monitoring information and EACM devices outside of its established ESPs, increasing the likelihood of compromised information and devices. URE did have protections in place to mitigate the potential risk. The devices in question were located within a restricted area with some physical security controls in place, including security cameras that monitored the area 24 hours a day, seven days a week, and card access systems that provided logging and monitoring. The MSSP provided URE with a description of the security controls in place to protect the affected EACM devices from unauthorized access, including, among other things, training for MSSP personnel and testing to ensure that changes and updates did not degrade security controls.

CIP-005-1 R1 SERC2012011010[10]

CIP-005-1 R1 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a Compliance Audit of URE. During the Compliance Audit, SERC discovered URE failed to identity field devices serially connected to an ESP as access points to the ESPs. Additionally, URE employs intrusion detection systems (IDS) using network span (or mirror) ports which cross the ESP, providing another type of "communication" link, the endpoints of which must be considered access points to ESPs.

URE utilized field devices that are serially connected to modems that communicate and ultimately terminate at a CCA located inside of the ESP. The serial devices use asynchronous and non-routable communication that is converted into a digital format at the CCA (a communication front-end processor). Therefore, this configuration requires the identification and documentation of an access point to an ESP pursuant to CIP-005 R1.

[10] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

Additionally, URE had implemented IDS devices that use network switched port analyzer (SPAN or mirror) ports to transfer network traffic to the IDS devices for analysis. URE configured these ports only to monitor network traffic. For all communication endpoints terminating at any device within an ESP, however, an access point must be identified. URE did not identify the connection across the ESP boundary as an access point. Since the configuration did not allow any external communication to come into the ESP via the SPAN port, and only permitted data to flow out of the ESP, URE believed that it did not need to identify an access point. Despite this configuration, however, URE should have identified access points for this connection to the ESP.

SERC determined that URE was in violation of CIP-005-1 R1 because URE failed to identify and document the ESPs and all access points to the ESPs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until the present. URE's mitigation plan for this violation is intended to create a new hierarchal network architecture based upon industry standards for data centers, eliminate the SPAN ports, and prepare URE for compliance with the controls required by CIP-005-5.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The unidentified field devices were serial devices that did not use a routable protocol, and the network switched port analyzer was configured to monitor network traffic only. URE had procedural controls in place for ESP access point management, logging, monitoring, and change control and testing of significant changes. The ESPs where the devices resided utilized real-time monitoring, including an IDS.

CIP-005-1 R2: R2.2 (SERC201000730)[11]

CIP-005-1 R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

[11] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

CIP-005-1 R2 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE. SERC included an audit detail letter in which SERC notified URE that CIP-005-1 R2 would be in scope during the scheduled Spot Check.

SERC's Spot Check team reported that URE enabled ports and services at ESPs that were not required for normal or emergency operations or monitoring, a violation of CIP-005-1 R2.2. URE's access control lists contained the justifications for open ports and services for the sampled EACM devices. Based on its review of these lists, SERC determined that URE had enabled ports and services at the ESPs that were not required for operations or monitoring, or which the source or destination did not require. Specifically, URE configured one access point, a firewall, to allow a CCA, to connect to any destination outside of the ESP without a service restriction. The documented description of the configuration stated that a "review of that access rule was needed."

SERC also determined that one of the firewalls at a URE facility allowed any URE employee with Virtual Private Network (VPN) access to connect to any destination within the facility's ESP via a network basic input/output system or the programmable logic controllers (PLC) communications port. URE failed to demonstrate why the ports and services associated with these types of access were required for normal and emergency operations and monitoring.

SERC determined that although not fully implemented, URE did have documented policies and procedures requiring it to enable only ports and services required for normal and emergency operations and monitoring. SERC determined that URE was in violation of CIP-005-1 R2.2 because at certain access points to its ESPs, URE failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, and failed to document, individually or by specified grouping, the configuration of those ports and services.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed to ensure that it enabled only ports and services required for normal and emergency operations on access points to the ESP. This could have allowed unauthorized individuals or malware intended to exploit these ports and services to establish a connection inside the ESP, potentially disrupting operations. URE has two violations included in this Settlement Agreement that contributed to the elevated risk. The first was URE's failure to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls on all CCAs and non-CCAs (SERC201000678). The second was URE's failure to disable ports and services not required for emergency and normal operations on 174 Cyber Assets located inside an ESP (SERC201000730). URE did have protections in place to mitigate the potential risk. URE uses an access control model that denies access by default.

CIP-005-1 R3: R3.2 (SERC2012011011)[12]

CIP-005-1 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at

[12] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-1 R3 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a Compliance Audit of URE (Audit). During the Audit, SERC discovered a violation of CIP-005-1 R3. URE failed to implement either an electronic or a manual process for monitoring or logging access at access points to the ESP 24 hours a day, seven days a week.

URE had six firewalls located at a single facility configured to log electronically all access attempts, configuration changes, and other high-level functions. However, due to high rates of firewall processing and filtering, the firewalls were not logging authorized and unauthorized access attempts to the ESP.

SERC determined that URE was in violation of CIP-005-1 R3.2 because it did not implement an electronic or manual process for monitoring and logging access at access points to the ESP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintains a contract with a third-party security vendor that provide security analysis and prevention services at all times. The security vendor has monitoring devices at URE to assist in real-time monitoring of the URE ESP and is constantly monitoring the URE network for malicious activity. This includes immediate notification of detected security anomalies. Therefore, any malicious attempts on the firewalls would be subject to scrutiny despite the absence of authorized access

logging. Despite not logging for access, the firewalls were logging for configuration changes and protocol-based traffic denials, thereby providing the ability to detect and respond to malicious activity affecting the firewalls.

CIP-006

The purpose statement of Reliability Standard CIP-006 provides: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1.1 (SERC201000682)[13]

CIP-006-1 R1 provides:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

[13] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R1. Not all Cyber Assets located within an ESP resided within an identified PSP for two facilities.

On July 15, 2010, FERC approved an interpretation of CIP-006-2 R1.1 documenting a registered entity's ability to use alternate physical or logical measures to control physical access to Cyber Assets where the registered entity cannot establish a six-wall border. This interpretation included that the registered entity must submit a Technical Feasibility Exception (TFE) request that details the alternate physical or logical measures that protect the Cyber Assets.

SERC reviewed URE's physical security plans for the facilities in question and determined that the plans did require that all Cyber Assets within an ESP reside within an established secured PSP. The physical security plans did not specifically mention network cabling.

SERC learned that URE deployed alternative measures by enclosing portions of the network cabling in continuous steel conduit where it could not establish a six-wall border. URE also located the sections of the network cabling not enclosed in a conduit in a cable tray suspended above the ceiling of a hallway. Additionally, the building where the cable was located did have limited access, despite not being an identified PSP. URE failed to file a TFE documenting these alternative measures used to protect the communication links.

SERC determined that URE was in violation of CIP-006-1 R1.1 because URE failed to document alternative measures to control physical access to the Cyber Assets (network wiring) where it could not establish a six-wall border.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE filed the TFE.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had physical security controls in place, including limited access and video surveillance to the areas where the cabling is located. A metal conduit encloses the cabling, which would reduce the likelihood of physical or electronic access. The remaining cable was in a cable tray that is above the ceiling and out of plain sight.

CIP-006-1 R1 (SERC201000731)[14]

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE. In the audit detail letter, SERC notified URE that CIP-006-1 R1 would be in scope during the scheduled Spot Check.

The CIP Spot Check team reported a violation of CIP-006-1 R1. URE did not ensure that all the access points through each PSP were identified and did not ensure that the physical security plan reflected the actual PSP configuration.

URE had a physical security program in place prior to the mandatory and enforceable date of the Standard. This plan required a documented physical security assessment for each facility with CCAs. SERC staff reviewed the physical security assessment for two operating centers and determined that the assessment identified five access points into one of the operating centers, three into the center's

[14] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

storage area network server room, and six into the other operating center. SERC reviewed URE's PSP drawings, compared them to the applicable physical security assessment, and determined that URE failed to identify accurately and consistently the PSPs and all access points.

Specifically, SERC identified two instances where an access point to a PSP was undefined, undocumented, and without documented control measures approved in the physical security plan. In addition, the audit team identified that the physical security plan incorrectly identified a PSP boundary wall.

SERC determined that URE was in violation of CIP-006-1 R1 because URE failed to ensure identification of all the access points through each PSP, ensure that the physical security plan reflected the actual PSP configuration, and have measures in place to control entry to an identified PSP access point.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE identified all access points, the physical security plan reflected the PSP configuration, and URE put measures in place to control entry to identified access points.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify all access points correctly could result in a failure to protect each access point. Failing to ensure that the physical security plan reflects the actual PSP configuration could result in the inability to implement a secure PSP and secure PSP practices. URE did have protections in place to mitigate the potential risk. URE monitors physical access using security guards and cameras and secured the facilities in question with access controls and layers of security, including card readers at the main entry points to the building and at the top of the stairwell leading to the entry to the basement PSP.

CIP-006-1 R1 (SERC2012010586)[15]

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating it had a violation of CIP-006-1 R1. While conducting a physical security walk-down of its Critical Assets, URE identified two non-secured windows measuring greater than 96 square inches, one each at two separate sites. The window at one site was equipped with glass breakage detectors and alarms to URE's operation center. These detectors and alarms were in place since the Standard become mandatory and enforceable on URE. At the second site, the

[15] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

windows were located three stories above ground and were not easily accessible. URE, however, failed to identify these windows as PSP access points.

SERC determined URE had a violation of CIP-006-1 R1 for failing to identify all the access points through each PSP, ensure that the physical security plan reflected the PSP access points, and have measures in place to control entry to the PSP access points in question.

SERC determined the duration of the violation to be from when the Standard become mandatory and enforceable on URE through when URE had secured both windows so that they are no longer operable and/or did not measure greater than 96 square inches.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify all access points correctly could result in a failure to protect each access point. Failing to maintain an accurate physical security plan could result in the inability to implement a secure PSP and secure PSP access practices, and to secure the CCAs residing inside. URE did have protections in place to mitigate the potential risk. One window was three stories above the generating units and not easily accessible, and the window was equipped with glass breakage detectors that would trigger alarms if the glass was broken. In addition, URE monitors physical access at all times by using security guards and cameras.

CIP-006-1 R1: R1.8 (SERC2012010860)[16]

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8. URE reported that system complexity and implementation concerns regarding a system upgrade to URE's physical access control system (PACS) resulted in a system upgrade delay.

Specifically, URE failed to maintain a physical security plan that afforded all of the protections set forth in CIP-006-1 R1.8 to the URE PACS, which authorized or logged access to PSPs. URE failed to afford the protections of CIP-004-3 R3 by granting electronic access to two PACS administrators who had not been subject to the required PRA process. URE failed to afford the protections of CIP-007-3 R5.3.3 by failing to change the system control and account passwords within the specified period. URE failed to afford the protections of CIP-007-3 R2.1 by failing to document and implement a process to ensure it enabled only those ports and services required for normal and emergency operations. Specifically,

[16] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The pertinent language of the Requirement remained the same in each version.

URE opened ports and services related to remote management software to enable vendor support, but this support was not necessary for normal or emergency operations and URE did not document the justification. URE failed to afford the protections of CIP-009-3 R2 when it failed to test the physical security system disaster recovery plan for the calendar year. URE had tested this plan the year prior and the year after the missed testing. URE has not filed any TFEs for the PACS devices at issue in this violation.

SERC determined that URE had a violation of CIP-006-1 R1 because URE failed to create and maintain a physical security plan, approved by a senior manager or delegate, which ensured that Cyber Assets used in the access control and monitoring of the PSPs were afforded the protective measures specified in CIP-006-1 R1.8.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to ensure protection of Cyber Assets used in the access control and monitoring of the PSP could introduce additional vulnerabilities in the devices. In turn, the security of physical access points is degraded, potentially allowing unauthorized individuals to gain physical access to CCAs protected within PSPs. However, URE did have protections in place to mitigate the potential risk. The two administrators granted electronic access to the PACS without PRAs did undergo preliminary screening; this preliminary screening included a criminal history check and other checks designed to prevent potential risks posed by those individuals. The two individuals were and are in good standing with the company. The passwords that were not changed annually did meet the length requirements in CIP-007 R5.3 and URE had filed a TFE for its inability to technically meet the complexity requirements.

CIP-006-3c R1: R1.6.1 (SERC2013012360)

CIP-006-3c R1 provides in pertinent part:

> R1. Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> *****

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

CIP-006-3c R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-3c R1 for failing to log visitor access into a single PSP at two different times.

A contractor with authorized unescorted PSP access brought two visitors into the PSP at different times and failed to log their access. The issue was identified the following day when the contractor admitted that he failed to properly log the escorted visitors. The manual log used for tracking visitors at the time of the violation shows three manual entries. One entry the aforementioned contractor showed an entry at 8:30 a.m. and an exit at 2:30 p.m. The manual log entries, however, were non-sequential. In the course of its investigation, SERC discovered that the contractor made this entry in the manual log the day after escorting the visitors into the PSP.

URE provided an approved physical security plan, including provisions for visitor access management covering the two operating center facilities (the control centers). The plan requires escort of all visitors at all times while within the two operating centers. Additionally, the plan requires recording all visitor access to the PSP electronically or manually. URE reviewed both the electronic and manual logs associated with the access control and monitoring devices to the PSPs in question and discovered no other incidents.

SERC determined that URE had a violation of CIP-006-3c R1.6.1 for failing to log (manual or automated) the entry and exit, including the date and time, of visitors to PSPs.

SERC determined the duration of the violation to be from when the visitors came onsite through when the visitors left the site.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The contractor at issue did have valid access to CCAs and training on the documented visitor escorting policy. The contractor did escort the visitor while the visitor was in the PSP. URE's PSPs were secured with access controls, including electronic card readers at all access points, a security desk with guards at the main entrances to the buildings, and live 24 hour a day, seven day a week security cameras covering the areas. After reviewing other logs and video surveillance, URE determined that all other visitors to PSPs were properly escorted.

CIP-006-2 R3 (SERC201000679)[17]

CIP-006-2 R3 provides: "Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter."

CIP-006-2 R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-2 R3. A single firewall used to protect the facility's dispatch control call center ESP was not physically located within a designated PSP.

This issue involved a single firewall that was responsible for securing and monitoring CCAs in the operating center. That firewall was located outside of the designated PSP, the communication room of the operating center. URE had an established and approved physical security plan that enforced proper use of all Cyber Assets used in the access control and monitoring of the ESP and required them to reside within an identified PSP. Physical access control devices (i.e., card readers and cameras) protected the firewall in question, which was located in an area restricted from unauthorized personnel. However, URE had not designated this restricted area as a PSP in its physical security plan. URE granted access to this area based on job function and restricted access to a subset of approximately 10 information technology (IT) support personnel in the operations center. The 10 IT support personnel that had access to the restricted area each had a completed PRA on file and had completed annual cyber security training.

[17] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. This requirement did not exist in Version 1. The language of the Requirement remained the same in each version.

Through a physical walk-down and a review of operating center and plant diagrams, URE confirmed that all other electronic access control and monitoring systems resided within identified PSPs, and that this condition did not exist in any other areas of URE.

SERC determined that URE was in violation of CIP-006-2 R3 for failing to position all Cyber Assets used in the access control and/or monitoring of the ESP in an identified PSP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable through when URE relocated the firewall to a designated PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The single firewall in question was located within a restricted area that did have physical security controls in place, including security cameras that monitored the area 24 hours a day, seven days week and card access systems that provided logging and monitoring. Access to the firewall was limited to approximately 10 trained and screened IT administrators.

CIP-006-2 R3 (SERC201000733)[18]

CIP-006-2 R3 has a "Medium" VRF and a "Severe" VSL.

During a Spot Check of URE, SERC discovered a violation of CIP-006-2 R3. URE did not ensure that all ESP EACM devices resided within a defined PSP.

SERC discovered that URE contracted with a third-party MSSP to collect, identify, validate, and escalate events and monitor access points to URE's ESPs. The MSSP did so by locating certain monitoring devices at URE's facilities. Those monitoring devices would gather information and securely send it to the MSSP's central servers that were not located at URE's facilities. Because of this arrangement, the devices located at URE's facilities and the MSSP's central servers are EACM devices and must be protected pursuant to the applicable CIP Reliability Standards, including CIP-006-2 R3. URE's contract with the MSSP did not ensure that the MSSP's devices used in the access control and monitoring of URE's ESPs resided within an established PSP, as required by CIP-006-2 R3.

In addition to URE's failure to ensure contractually that the MSSP located the EACM devices within a PSP, URE also failed to provide evidence that the EACM devices in fact were located within a PSP. Specifically, SERC determined that the servers used for management of access points to ESPs were not

[18] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

located within an established PSP. URE did have a procedure that required identification of EACM devices and required them to be located within PSPs. URE, however, failed to implement this procedure with respect to these EACM devices.

In addition to the MSSP's EACM devices, SERC also determined that URE failed to locate some of its own EACM devices within a PSP, as required by CIP-006-2 R3. The EACM devices at issue were servers used to configure access points to ESPs and manage firewalls and routers.

SERC determined that URE was in violation of CIP-006 R3 because it failed to provide evidence that Cyber Assets used in the EACM of the ESPs were located within a PSP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through the present.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that some devices involved in the access control and monitoring of an ESP were located within a defined PSP increased the risk of unauthorized physical access to URE's EACM devices. URE did have protections in place to mitigate the potential risk. The devices at issue were located within a restricted area with some physical security controls in place, including security cameras that monitor the area 24 hours a day, seven days a week, and card access systems that provided logging and monitoring. The third-party MSSP provided URE with a description of the security controls in place to protect the EACM devices from unauthorized access. MSSP trained its personnel and performed testing to ensure that changes and updates did not degrade security controls.

CIP-006-1 R4 (SERC2012010585)[19]

CIP-006-1 R4 provides:

> R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

[19] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

CIP-006-1 R4 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R4 because URE did not have a manual log to record the use of an equipment elevator that served as an access point to one PSP.

URE conducted a physical security walk through of the URE operating center and determined there were no manual logging mechanisms implemented to record use of the equipment elevator lobby double doors, which is an established access point to the PSP there. Seventy individuals had access to this area during the time of the violation.

SERC determined that URE was in violation of CIP-006-1 R4 because it did not implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to secure access points to the PSP could have allowed unauthorized personnel unescorted access without detection. URE did have protections in place to mitigate the potential risk. URE did have an alarm contact on the doors located under the equipment hatch that alarms to the URE monitoring and notification center any time the equipment elevator is used. When not in use, the elevator is located at ground level outside the PSP, and the only way to access it is through the PSP. There is a card reader located at the PSP access point which grants access to the telecommunication room where networking CCAs are located. There is an armed response team on-site 24 hours a day, seven days a week.

CIP-006-3a R4 (SERC201000683)

CIP-006-3a R4 provides:

> R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> - Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
> - Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-3a R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it had a violation of CIP-006-3a R4 because the doors to its server room and operations center were inadvertently left unlocked for approximately 7 hours and 15 minutes after a fire drill.

URE had a scheduled fire drill. At the time, in accordance with URE's physical security plan, the door locks were programmed to fail open for safety reasons in any fire drill or other emergency-related event. It was URE's standard practice to reset the alarms and locks after the completion of the drill. In this instance, the responsible individuals failed to reset the door locks to the PSP at the conclusion of the fire drill.

URE reviewed video footage and access logs to determine that the doors to the server room and operations center were unsecured for 9 hours and 19 minutes, which included the duration of the fire drill and 7 hours and 15 minutes after the drill. URE also found that two contract individuals had accessed the PSP without proper authorization during this period. The individuals at issue were

performing maintenance on lighting fixtures, and had general access into the building, but did not have authorized access into the operations center PSP. URE normally escorted these individuals into the controlled area, but in this instance, the individuals entered the PSP after scanning for badge access that was denied. The individuals' badge attempt was logged and an alarm was generated, but it was not received and responded to immediately due to the ongoing fire drill efforts.

URE had a physical security plan that required, in the event of a system failure of a PACS, the monitoring and notification center to restrict access to the PSP. However, in this instance, access was restricted only for the duration of the fire drill by placing security guards at the entry points.

SERC determined that URE was in violation of CIP-006-3a R4 for failing to implement the operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from 10:02 a.m., when the drill started and URE failed to manage physical access at all access points to the PSPs through 7:21 p.m. when URE reset the locks at the access points to the PSP at issue.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, a failure to implement technical and procedural controls resulted in unauthorized access into the PSP at issue. Unauthorized access into a PSP could allow potential unauthorized access to the CCAs contained inside the PSP. URE did have protections in place to mitigate the potential risk. URE had multiple cameras with recorded video feeds monitoring the server room and operations center during the violation, including the scheduled fire drill and the period after the drill. URE's electronic logging was enabled and functional during the violation, including the scheduled fire drill and the period after the drill. The contractors at issue had undergone background checks and were approved for general access into the facility, although not to the CCAs within the PSP. URE's security guards visually monitored the area during the drill. No Cyber Assets within the PSP were compromised.

CIP-006-3c R6 (SERC2012009109)

CIP-006-3c R6 provides:

> R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural

mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

CIP-006-3c R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-006-3c R6. URE failed to record or to maintain logs of an unauthorized employee's physical access.

URE discovered that a vendor-provided custodial employee was attempting to gain entry to a card-access and biometric-controlled control center PSP with a second individual's badge. The second individual loaned the access badge to the first individual while on vacation. URE's PACS logged a biometric mismatch for the actual cardholder. URE immediately responded to the alarm, and one of URE's security personnel confiscated the badge.

This instance prompted URE to conduct an internal investigation. URE reviewed historical video surveillance and electronic and manual logs to determine the full extent of the unauthorized access attempts. During the investigation, URE determined that the vendor-provided custodial employee had also entered the control center PSP, without a valid access card. Personnel within the PSP allowed the individual inside after the individual requested access locally after his or her attempt to use the access badge failed. URE did not record and maintain manual logs of this individual's physical access since the individual was not properly escorted in the PSP in accordance with the established visitor control program.

URE had a physical security program established for addressing all CIP physical security measures. The program applies to all URE facilities and personnel and requires all URE facilities containing assets subject the CIP Reliability Standards to document a physical security plan. Additionally, URE's program requires continuous escorting of any individual without authorized unescorted physical access to a PSP,

including specific logging of the visitor's name, date, and time of entry and exits. URE also had procedures requiring it to log and monitor access to PSPs 24 hours per day, seven days per week.

SERC determined that because URE did not record or maintain logs of a vendor employee's physical access, URE did not record sufficient information to identify uniquely the individual and the individual's time of access to the URE PSP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be when the vendor employee gained access to the PSP without creating a manual log entry following a biometric mismatch and URE security personnel confiscated the badge with which the vendor employee was attempting unauthorized access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The vendor employee had undergone URE's cyber security awareness training prior to accessing the PSP. URE had a biometric reader in place at the access point to the PSP that alarmed when the vendor employee attempted access with an incorrect badge. Additionally, following the biometric mismatch, URE's security personnel acted swiftly to confiscate the badge used during the access attempt. The PSP that the vendor employee entered was a control center manned and monitored 24 hours a day, seven days a week.

CIP-007

The purpose statement of Reliability Standard CIP-007 provides in pertinent part:

> Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-007-1 R1 (SERC201000678)[20]

CIP-007-1 R1 provides:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do

[20] URE's violation applies from Version 1 through Version 2 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R1. URE reported that its procedures ensured functional testing for significant changes to systems, but the associated testing did not include an assessment of cyber security controls.

URE's documented change management program, which was applicable to all CCAs and Cyber Assets located inside the ESPs, required testing of significant changes to all existing and new Cyber Assets located inside an ESP. URE revised the program to include CIP-007 R1 testing of significant changes to existing and new Cyber Assets. Upon these revisions, URE's processes and procedures required the testing of significant changes to existing Cyber Assets within the ESP to ensure that they do not adversely affect existing cyber security controls. URE's actual performance of testing cyber security controls was contingent on the installation of certain software, and URE did not implement this software until approximately 22 months after URE revised the program.

As a result, SERC determined that URE failed to test security controls for 142 CCAs (including workstations, servers, modems, switches, and routers) and 69 Cyber Assets located inside an ESP (including printers, workstations, servers, modems, and tape libraries) until URE implemented the software.

SERC determined that URE was in violation of CIP-007-1 R1 for failing to test significant changes to new and existing Cyber Assets within the ESP to ensure that they do not adversely affect existing cyber security controls. While URE did have policies and procedures in place that enforced testing of both

functional and security controls, it failed to test significant changes for adverse effects on existing security controls.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through when URE implemented software to enable it to test cyber security controls for CCAs and Cyber Assets.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to test cyber security controls prior to implementation in the production environment for an extended period could have introduced security vulnerabilities to critical and non-critical Cyber Assets located inside the ESP. URE did have some protections in place. URE had procedures in place for change control and testing of significant changes. URE did complete functional testing prior to implementation in the production environment, which reduced the risk of operational downtime. The ESPs, where the devices resided, utilized real-time monitoring, which included IDS.

CIP-007-1 R2 (SERC201000734)

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
> >
> > R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE. In the audit detail letter, SERC notified URE that CIP-007-1 R2 would be in scope of the scheduled Spot Check.

The CIP Spot Check team reported a violation of CIP-007-1 R2 because URE did not document the required ports and services for the sampled Cyber Assets within the ESP, and did not disable ports and services that were not required for normal or emergency operations.

SERC reviewed the results of the URE cyber vulnerability assessment (CVA) and determined that URE did not provide a baseline list for all required ports and services. The CVA showed that multiple open ports lacked justification for being open. Additionally, specific ports and services on control center devices were enabled but not required for normal and emergency operations. URE completed a full-scope assessment of the issue and found no baseline documentation for 211 devices (CCAs and non-CCAs). URE attested to 174 of those devices having ports and services enabled that were not needed for normal or emergency operations.

SERC determined that URE failed to enable only those ports and services required for normal and emergency operations. Specifically, URE did not provide evidence to support having enabled ports and services on all Cyber Assets, resulting in a violation of CIP-007-1 R2.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Failure to ensure that only ports and services needed for normal and emergency operations were enabled could allow unauthorized individuals or malware to exploit these ports, and thereby disrupt operations or gain unauthorized access to CCAs. URE has two violations included in this Settlement Agreement that contributed to the serious or substantial risk. The first violation was for URE's failure to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls (SERC201000678) on all CCAs and non-CCAs. The second violation was URE's failure to ensure that, at all access points to the ESP, only ports and services required for emergency operations and for monitoring Cyber Assets within ESPs were enabled (SERC201000730). URE did have some protections in place. URE had IDS devices in place inside the ESP and on the corporate network. URE used an access control model that denied access by default. URE had a third party performing security logging and monitoring. Finally, URE had processes and procedures in an attempt to ensure the proper management of ports and services on Cyber Assets located inside the ESP.

CIP-007-1 R3 (SERC201000735)[21]

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE.

URE's cyber security patch and vulnerability management program applies to all URE functions and all Critical and non-critical Cyber Assets within URE's ESP. Although URE reviewed this program annually, URE relied on procedural documents to provide the details of its security patch management program.

SERC reviewed one of URE's procedures, the URE control system procedure put in place to implement the URE cyber security patch and vulnerability management program. SERC determined that this procedure did not address the evaluation of patches within 30 calendar days of availability, testing of patches, and deployment of patches to several device types, as required by CIP-007-1 R3.1.

Additionally, SERC reviewed the URE patch evaluation list for some of URE's functions, provided during the Spot Check as evidence of URE's implementation of the procedures described above. This list

[21] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement changed from Version 1 to Version 2. The language of the Requirement remained the same from Version 2 to version 3. Version 2 removed the following words from R3.2: "…or an acceptance of risk."

showed multiple security patches released without a completed assessment or a documented mandatory installation date. The list did not include information regarding the patches' applicability or compensatory measures applied to mitigate risks in the event that a patch was not applied. The patch evaluation list showed evidence of the assessment of security patches for operating systems but did not show evidence of URE's assessment of security patches applicable to non-operating system software.

Finally, to evaluate URE's security patch management program for other functions, SERC reviewed URE's CVA, which indicated that URE failed to assess certain historical security patches applicable to Cyber Assets inside of an ESP and failed to apply them as necessary. The CVA results also indicated that URE failed to maintain documentation of security patch assessments and the associated software inventory required to support patch review as required by CIP-007-1 R3.2.

SERC determined that URE was in violation of CIP-007 R3 because it failed to provide evidence of an established security patch management program for evaluating and installing applicable cyber security software patches for all Cyber Assets within its ESPs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through the present.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to assess and install security patches could have resulted in unaddressed vulnerabilities for extended periods, increasing the risk of a successful intrusion. URE did have protections in place to mitigate the potential risk. The unassessed security patches were applicable to a limited number of non-critical Cyber Assets. All of URE's Cyber Assets resided within ESPs and PSPs. Access to Cyber Assets within the ESP from outside the ESP required two-factor authentication. During the violation period, URE's electronic access and control monitoring devices did not identify any malicious activity affecting the involved Cyber Assets.

CIP-007-3a R3 (SERC2012010883)

CIP-007-3a R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-007-3 R3 because URE failed to assess three operating system vendor advisories for applicability within 30 days of availability.

The three advisories identified in URE's Self-Report were applicable to devices with a specific operating system, limiting the issue to approximately 20 non-critical Cyber Assets out of 140 contained in the

associated ESP. The vendor-assigned vulnerability rating for these advisories was "High." The security patches associated with these advisories became available but URE did not assess them until approximately six months later, and did not document the assessment until approximately eleven months after the security patches became available. URE installed the three security patches approximately five months after URE documented the assessment. URE only installs assessed security patches during scheduled system outages, which typically occur twice a year. In this instance, URE failed to train adequately the administrator responsible for assessing these patches on the manual process for security patch assessment.

SERC determined that URE failed to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability and failed to document the implementation of such security patches.

SERC determined the duration of the violation to be from when the first security patch was available through when URE assessed the missing patches.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The security patches missed were applicable to a limited number of non-critical Cyber Assets. All of URE's Cyber Assets resided within ESPs and PSPs. Access to Cyber Assets from outside the ESP required two-factor authentication. URE's EACM devices did not identify any malicious activity during the violation period that would have affected the 20 non-critical Cyber Assets at issue.

CIP-007-1 R4 (SERC201000566)[22]

CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document

[22] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R4. URE identified a single server located inside the ESP that did not have anti-malware software installed. According to URE, the server did not support anti-malware software due to hardware resource restrictions. URE used the server for archiving historical data, and the server had no ability to control elements of the BPS.

URE's CIP-007 R4 anti-malware process in place at the time of the Self-Report addressed CIP-007 R4 and included a requirement to file a TFE in cases where URE could not install anti-malware. URE failed to submit a TFE for this server. This violation resulted from URE's failure to follow its established process.

SERC determined that URE was in violation of CIP-007 R4 because it failed to install malware and anti-virus protection tools or implement and document compensating measures on the identified device.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The server at issue was located inside a PSP and ESP and had no ability to control elements of the BPS. The other devices in the ESP had anti-malware software installed, which should have restricted the spread of malware in the unlikely event that the device became infected.

CIP-007-1 R4:4.2 (SERC201000736)[23]

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE.

[23] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version. However, beginning with Version 2, the phrase "or an acceptance of risk" no longer appeared in Requirement R4.1.

The CIP Spot Check team reported a violation of CIP-007-1 R4.2 because URE did not have a process for testing and installing antivirus and anti-malware "signatures" for all Cyber Assets.

URE first implemented a procedure for testing antivirus and malware prevention tools nearly six months after the date on which URE was required to comply with CIP-007-1 R4. This procedure addressed the antivirus and prevention tools used to address compliance with CIP-007 R4. This procedure required each URE strategic business unit (SBU) to create a process for the testing and installing of antivirus and malware signatures. However, URE failed to provide SBU processes for testing antivirus and malware prevention signatures.

URE also provided evidence of pattern testing conducted by the vendor to minimize adverse effects during the deployment of antivirus and malware signatures to that vendor's products. The evidence also described the vendor's antivirus definition certification process for verifying and validating signatures. SERC determined the vendor's performance of testing did not eliminate the need for URE do so.

SERC determined that URE violated CIP-007 R4.2 because it failed to document a process for the testing of antivirus and malware prevention signatures.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through the present.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did use antivirus software and other malware prevention tools on Cyber Assets located inside of the ESP, where technically feasible, excluding the device involved in the instant violation of CIP-007-1 R4 (SERC201000566). URE attested that it tested antivirus and malware signatures, prior to installation, on a development system that reflected the production system. URE did provide evidence of vendor testing of antivirus and malware prevention signatures prior to deployment.

CIP-007-1 R5 (SERC201000570)

CIP-007-1 R5 provides:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-1 R5 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report, stating that it was in violation of CIP-007-1 R5.2 because it failed to remove or disable 48 accounts. The 48 accounts in question existed on servers and workstations with various operating systems prior to the mandatory date of compliance. URE identified all of the account issues in an annual account review, which included all local accounts on all Cyber Assets located inside of an ESP. Some of the operating systems were equipped with controls to disable automatically accounts with 90 days of inactivity, resulting in all those accounts being disabled but not removed or deleted. The other operating systems were equipped with no such controls. URE removed all these accounts on the same day it submitted the Self-Report.

While SERC staff was performing its assessment and determining the scope of the violation, the following additional issues were reported:

1. During a CIP Spot Check, SERC made the following determinations:

    a. URE failed to remove, disable, rename, or change passwords for default accounts for three Cyber Assets prior to putting them into service. Additionally, URE did not require and use passwords for all accounts on all of its Cyber Assets within the ESPs. Lastly, URE did not change passwords annually for all accounts on Cyber Assets within the ESP.

    b. In at least one instance, a default password on an account existed prior to the mandatory date of compliance and had not been changed. Additionally, URE's CVA identified three systems that had default accounts with unchanged passwords. The CVA also identified systems with accounts no longer needed, including a Cyber Asset with a password that had not been changed since the mandatory date of compliance. The devices in question were servers and workstations that were capable of enforcing the password requirements of CIP-007 R5.3 and Ethernet modems that are infrequently logged into and not capable of enforcing the password requirements of CIP-007 R5.3.

c. URE had four administrative accounts with passwords older than one year because URE failed to change these passwords annually, as required. The passwords for the accounts were late by: 1) 135 days for account one; 2) 17 days for account two; 3) 7 days for account three; and 4) 48 days for account four.

2. URE submitted a Self-Report to SERC stating that 16 servers (14 CCAs and 2 non-critical Cyber Assets) were not configured to enforce the password requirements of CIP-007 R5.3. Although the servers were capable of enforcing the password requirements of CIP-007 R5, URE did not discover the failure to configure the passwords until 19 months after the mandatory date of compliance. As a result, SERC determined that URE failed to ensure that all Cyber Assets within its ESPs had passwords meeting the parameters of CIP-007 R5.3.

3. URE submitted a Self-Report to SERC stating that while performing its annual CVA as required by CIP-007 R8, it discovered non-compliant configuration files on a backup server. Specifically URE found that controls for technically enforcing the use of a special character were not in place. More specifically, the configuration option which specifies the minimum number of special characters required, was not enabled, allowing users to select a password that did not have a special character, as required by CIP-007 R5.3.2.

SERC determined that URE was in violation of CIP-007 R5 for failing to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to remove default accounts or change passwords on default accounts could have left Cyber Assets vulnerable to compromise since many default account credentials are public information. Failing to change passwords on an annual basis and failing to use strong password controls could leave passwords, and the systems they protect, susceptible to attacks potentially allowing an unauthorized user to access or compromise a system. URE did have protections in place to mitigate the potential risk. All devices were located in an ESP and PSP. URE's Cyber Assets reside behind firewalls and physically secured facilities with card readers and biometrics controls. The ESPs where the devices resided utilized real-time monitoring, including IDS that monitored the switch ports connected to the devices. Malware prevention and other security controls, such as patching, local firewalls, and antivirus software, remained operational and up-to-date for the period in question.

CIP-007-1 R6 (SERC201000567)

CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
> >
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
> >
> > R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
> >
> > R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it had a violation of CIP-007-1 R6. URE identified three Cyber Assets located inside an ESP that were not logging security events due to improper configurations and technical infeasibility. Two of the devices were servers that did not have the security logging software installed and configured properly.

The third device was an antiquated server used for the archiving of historical data and had no ability to control elements of the BPS. This device did not support the security logging client used by URE. Despite this, URE failed to file a TFE for the device. This server was in place prior to the mandatory date of compliance and was removed from operation approximately fifteen months after the mandatory date of compliance.

While SERC was performing its assessment and determining the scope of the violation, URE reported the following additional issues:

1. URE reported that it failed to configure some hosts to send security monitoring messages and to log such messages, as required. Specifically, URE failed to configure 12 out of 215 devices in an established ESP to send logs to the centralized server. In some cases, the security logging software was not installed and configured properly, and in others the centralized sever was not configured to receive logging data. SERC determined that URE failed to ensure that all Cyber Assets within the ESPs, as technically feasible, implement automated tools or organizational process controls to monitor system events related to cyber security.

2. URE reported that the centralized server was not processing cyber security logs for seven non-critical Cyber Assets. The systems were configured to log events locally and to send the logs to the server. The server was not configured properly to receive or monitor log events from the seven assets. URE discovered this issue during its annual review of the security monitoring controls. The improper configuration dated back to the earliest in-service date of the seven devices, and URE corrected the configuration approximately two years later.

3. URE reported that during two network upgrades, security logging and monitoring was unavailable for some critical and non-critical Cyber Assets. On two occasions, URE experienced a network outage that resulted in a failure of logging and monitoring for seven Cyber Assets. The two network outages resulted from the need to upgrade software for some URE network devices for both security and functional purposes. These network devices managed the connection of the seven Cyber Assets in question to the central logging server. During the two network upgrades, logging and monitoring was unavailable for a total of 120 minutes.

    a. The first outage lasted 30 minutes. Three Cyber Assets did not have complete redundancy and were not capable of storing logs locally for this period, resulting in a disruption in logging and monitoring for the three assets at issue.

    b. The second outage occurred approximately five months after the first outage and lasted 90 minutes. Four Cyber Assets were not sending logs to the centralized server and were unable to archive logs locally for the outage period, thus resulting in a disruption in logging and monitoring for the four devices at issue.

SERC determined that URE was in violation of CIP-007 R6 for failing to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events related to cyber security.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to monitor system events related to cyber security for its Cyber Assets within the ESPs could have resulted in a security breach going undetected. An undetected security breach may have rendered CCAs inoperable, resulting in the loss of monitoring and control of the BPS. URE's failure to retain logs related to security events could have impaired its ability to conduct an incident response. URE did have protections in place to mitigate the potential risk. The ESPs where the devices resided utilized real-time monitoring, which included IDS that monitored the switch ports connected to the devices. Malware prevention and other security controls remained operational and up-to-date for the period in question. Instances involving network outages were controlled events with trained technical personnel present for the entire duration of the outages and actively monitoring the system conditions. URE reviewed all firewall logs and found no unauthorized access or access attempts.

CIP-007-3a R8 (SERC2012011013)

CIP-007-3a R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
>
> R8.3. A review of controls for default accounts; and,
>
> R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-3a R8 has a "Lower" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE.

During the Audit, SERC determined that URE had violated CIP-007-3a R8.2 and R8.3 because URE did not perform a CVA of all Cyber Assets within the ESP at least annually, as required. Specifically, URE had excluded network switches and routers from aspects of its CVA.

URE performed CVAs for devices, however, URE's evidence did not demonstrate the review of all enabled ports and services on network routers and network switches within the ESP as required by CIP-007-3 R8.2.

Additionally, URE did not fully perform a review of controls for default accounts on switches and routers within the ESP as required by CIP-007-3 R8.3. URE stated that it used the same default account reviews as performed for Electronic Access Points (EAPs), pursuant to CIP-005-3 R4.4. However, the scripts provided for the EAPs had been hard coded with account names specific to the firewalls. Therefore, these scripts were inadequate for discovering default accounts on the network switches and stand-alone routers.

SERC determined that URE was in violation of CIP-007-3a R8.2 and R8.3 because it did not perform a CVA for all Cyber Assets within the ESP. Specifically, URE did not demonstrate that it reviewed ports and services required for operations, or review controls for default accounts for all Cyber Assets within the ESP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Despite URE's inability to substantiate a review of ports and services enabled on network switches and routers residing inside the ESP, the switch configurations make the ports and services incapable of logical port filtering. URE performed a complete CVA of all electronic access points, ensuring that its ESP's perimeter defenses were properly hardened. While URE did not perform a review of controls for default accounts on the network switches and routing devices residing inside the ESP, a malicious attacker attempting to exploit said devices would have had to cross the electronic access point firewall perimeter defenses first. URE maintains a contract with a third-party security vendor that provides security analysis and prevention services at all times. The security vendor has monitoring devices to assist in real-time monitoring of the URE ESP and constantly monitors the URE network for malicious activity. The vendor's monitoring also includes immediate notification of detected security anomalies.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE self-reported 17 of the violations, which SERC considered a mitigating factor;
2. URE was cooperative throughout the compliance enforcement process, which SERC considered a mitigating factor;
3. URE had an internal compliance program (ICP) at the time the violations occurred, which SERC considered a mitigating factor;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-007-1 R1 and R2 (SERC201000678 and SERC201000734) posed a serious or substantial risk to the reliability of the BPS, as discussed above;
6. in addition to paying the monetary penalty, URE agreed to:
    a. Implement certain physical security measures beyond those required to comply with the applicable NERC Reliability Standards. URE installed revolving doors designed to prevent tailgating at the outermost entry points at the facility housing its control center, a data center, and its security-monitoring center. URE also installed high-resolution surveillance cameras to enable earlier detection of events and enhanced forensic work after an event. URE implemented biometric identity authentication tools; and
    b. Implement a training and awareness program that exceeds the requirements of the applicable NERC Reliability Standards. This program includes a professionally developed computer-based interactive training that is required of all employees, not just those with access to CCAs. URE ensures awareness of security issues through regular communications, posters, tips, and alerts.
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of two hundred fifty thousand dollars ($250,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[24]

CIP-002-2 R2 (SERC201000685)

URE's Mitigation Plan to address its violation of CIP-002-2 R2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005822-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the scoping workshop checklist to address new construction and modifications at existing Critical Asset facilities;
2. revise the risk-based assessment methodology to require reissuance of the Critical Asset list after the commissioning of new Critical Assets; and
3. update the Critical Asset list.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. the newly revised and updated scoping workshop checklist;
2. the new RBAM procedure; and
3. a copy of the Critical Asset list update letter.

CIP-004-1 R3 (SERC201000568)

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005271-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove physical access;
2. implement a process to include at least two reviewers during quarterly reviews; and

[24] *See* 18 C.F.R § 39.7(d)(6).

3. implement a process to conduct daily reviews of physical access changes to PSPs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. the request to remove the individual from the access system;
2. confirmation of removal completed; and
3. evidence of the establishment of the daily review process showing the reoccurrence of the monthly review process and examples of the daily report.

CIP-004-1 R4 (SERC201000569)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005273-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove accesses and documented changes as required;
2. review local and centralized accounts during the quarterly review;
3. implement detection reporting process to detect and report configuration changes to ensure no local accounts are added without authorization and all account changes are documented using the business unit's change management process and reviewed and approved by the change control board prior to being executed;
4. formalize procedural steps for documenting physical access changes;
5. implement a daily review of the human resources system change report, which identifies job changes and organizational changes for personnel across the entire entity and updates the master list as needed on a daily basis;
6. implement a process for IT security to review the daily human resources termination review report for any changes affecting access lists and forward such information to the appropriate business unit; and
7. train access control employees and took steps to ensure awareness of regulatory timelines for access removals and documentation of access removals.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. change request to remove cyber access for the individual in question;
2. quarterly review notice;
3. training roster for access control personnel;
4. checkout procedure explanation communicated to targeted personnel;
5. HR termination report;
6. add/remove report;
7. job change report;
8. employee checkout procedure;
9. access control procedure; and
10. Configuration change monitoring report example.

CIP-004-3 R4 (SERC2012010884)

URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008635 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. execute an intergroup agreement allowing senior executives to be granted access to CCAs, provided that such individuals meet the PRA and training requirements; and
2. notify authorized individual that access to this PSP had been granted to the involved individuals pursuant to this intergroup agreement.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a copy of the intergroup agreement.

CIP-005-1 R1; R1.5 (SERC201000729)

URE's Mitigation Plan to address its violation of CIP-005-1 R1; R1.5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is

designated as SERCMIT010429 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. gather functional requirements for a new, locally managed, Security and Event Management (SIEM) system;
2. complete the project scope development and detailed project plan for the new SIEM system implementation;
3. review the SIEM devices to ensure that new devices provide full coverage leaving no gaps in the monitoring system;
4. determine EACM device placement;
5. install all new hardware to ensure that new SIEM system is ready for testing;
6. conduct testing to ensure full functionality of new SIEM system; and
7. complete installation of new SIEM system and provide any necessary training.

CIP-005-1 R1 (SERC2012011010)

URE's Mitigation Plan to address its violation of CIP-005-1 R1was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010430 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. meet with project manager (PM) to verify schedule;
2. implement Phase I of network and installation of infrastructure;
3. run Phase I systems in parallel for testing;
4. complete Phase I network cut-over;
5. meet with PM to verify schedule for Phase II;
6. implement Phase II of network and installation of infrastructure;
7. complete Phase II network cut-over;
8. eliminate SPAN ports through network re-architecture project;

9. review Project Scope for completion;
10. transition CIP-005 governance to comply with controls provided in CIP 005-5 and adoption of revised definitions for "Electronic Access Point," "External Routable Connectivity," and "Electronic Security Perimeter;" and
11. review ESP diagrams and revise to align with CIP-005-5 governance.

CIP-005-1 R2; R2.2 (SERC201000730)

URE's Mitigation Plan to address its violation of CIP-005-1 R2; R2.2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010422 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the rule at issue to restrict inbound network access;
2. remove VPN access through the facility's firewall; and
3. ensure that firewall configurations would be reviewed annually in the annual CVAs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. a change ticket as evidence of the configuration change to remove the rule at issue to restrict inbound access;
2. an email from the subject matter expert attesting to the fact that VEPN access was removed; and
3. a CVA procedure which specifies that a review of ports and services at access points is reviewed as part of the CVA.

CIP-005-1 R3; R3.2 (SERC2012011011)

URE's Mitigation Plan to address its violation of CIP-005-1 R3; R3.2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010424 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace and configured new firewalls to generate adequate logs;
2. update all related network drawings, ESP drawings, and asset inventories to reflect the firewall replacements;
3. update CVA procedures to ensure that a CVA is conducted to review firewall configurations.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. two screenshots showing that the new firewalls that could robustly handle the logging requirements were logging;
2. updated network drawings, ESP drawings, and asset inventories; and
3. an updated CVA procedure that addresses the annual review of electronic access points.

CIP-006-1 R1.1 (SERC201000682)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005283-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an assessment of the current locations of each access control system communication lines between PSPs at its facilities;
2. continue with cutover project. This will move control system components and communications from the corporate network to a URE control system network, further isolating the control system;
3. verify that the unprotected routable network cables outside a PSP will be protected by running it through steel conduit; and
4. file a TFE and implement compensating measures as stated above. The primary first line of protection is the steel conduit enclosures that protect the communication networks. These are also contained in an area of the plant that has very limited access with other physical protections in place.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. independent third-party assessment of the facilities in question;
2. schedule review of network changes and cutover schedule;
3. mitigation schedule;
4. copy of work order necessary for conduit enclosure completion; and
5. photo of the type of conduit enclosing the cables in two facilities.

CIP-006-1 R1 (SERC201000731)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010393 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. secure the hole in the wall to less than a 96 square inch opening by securing a steel bar horizontally across the opening; and
2. update the PSP drawings in the physical security plan to reflect the proper PSP perimeter was completed.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. a photo showing the opening was closed with horizontal bars that reduced the opening to less than 96 square inches; and
2. an edited version of the PSP drawing for the area in question.

CIP-006-1 R1 (SERC2012010586)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007759-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct physical security walk-downs at all Critical Assets to ensure that all access points have the appropriate security measures in place to control access to the PSPs; and
2. secure operable windows to render them inoperable or smaller than 96 square inches.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. photos showing riveting shut of the operable windows to the fixed frames in the PSP in question and a statement noting completion; and
2. photos showing screening of the operable windows and an email statement noting completion.

CIP-006-1 R1; R1.8 (SERC2012010860)

URE's Mitigation Plan to address its violation of CIP-006-1 R1; R1.8 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008652-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove access to the PACS;
2. establish and populate a new active directory security group for administrators that requires an individual to have a valid PRA prior to being added to the directory;
3. change the system control and account passwords;
4. stop and disabled unnecessary ports and services;
5. uninstall software associated with unnecessary services during approved outage window; and
6. update the disaster recovery test plan, execute test plan, and schedule the next disaster recovery test plan.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. properties shown for creating a new group with proper PRAs and written explanation of emails previously submitted;

2. IT tickets showing the disabling of ports and services identified during pre-audit review as no longer required for system operation;
3. disaster recovery plan showing an updated recovery test plan;
4. four additional emails showing scheduled reviews; and
5. work-request documentation for "password reset."

CIP-006-3c R1; R1.6.1 (SERC2013012360)

URE's Mitigation Plan to address its violation of CIP-006-3c R1; R1.6.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009616 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke the contractor's access to the PSP at issue;
2. retrain the contractor on the facility's visitor management policy;
3. issue a security awareness bulletin on the existing visitor management policy to all personnel with unescorted access to the PSP at issue; and
4. review the existing visitor management policy with all employees with unescorted access to the PSP at issue.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. a training roster showing the contractor retraining was complete; and
2. a copy of a security awareness bulletin that was distributed to all personnel within the business unit.

CIP-006-2 R3 (SERC201000679)

URE's Mitigation Plan to address its violation of CIP-006-2 R3 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005290-1 and was submitted as non-public information to in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. relocate the firewall at issue into a defined PSP; and
2. modify the design change notice procedures to include a security review of all hardware additions and modifications, thereby preventing future access control devices from not being located in a PSP.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. firewall compliance report (before and after)
2. work order detailing work and completion;
3. system test plan to verify operability after completion; and
4. revision that illustrates cyber security checkpoint when making system changes.

CIP-006-2 R3 (SERC201000733)

URE's Mitigation Plan to address its violation of CIP-006-2 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010428 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete conceptual design for the project and determine necessary resources to complete the project;
2. develop preliminary physical protection specifications required for the physical space selected;
3. review completed physical design details during an on-site meeting and walk down and review all final design drawings (physical) and final project specifications;
4. review physical engineering design changes and determine any environmental effects;
5. start necessary field construction work;
6. verify construction progress has reached the scheduled halfway point;
7. perform acceptance testing to ensure the installation is functional, complies with design specifications, and is within scoping requirements;
8. document functional testing; and

9. close all outstanding work orders associated with the project.

CIP-006-1 R4 (SERC2012010585)

URE's Mitigation Plan to address its violation of CIP-006-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007760-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install card readers and alarm contacts on equipment lift vestibule double doors to provide for logging and monitoring of PSP access point; and
2. modify physical security plan to redefine PSP to remove equipment lift as an access point and identify vestibule double doors as a new access point.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. card reader access request and reader access system test; and
2. security plan with updated PSP drawing.

CIP-006-3a R4 (SERC201000683)

URE's Mitigation Plan to address its violation of CIP-006-3a R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007581 and was submitted as non-public information to in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. modify the configuration of the access point to the PSP at issue to ensure that doors would remain locked during fire drills;
2. modify alarm response procedures to require physical verification of functionality of locks prior to clearing alarm;
3. add check of functionality of physical access control systems to post-fire drill procedures; and
4. train building security personnel on required steps after a fire drill.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. documentation of verification that doors remain secure during fire alarm testing;
2. Email with new alarm verification process explained in detail;
3. Copy of building emergency response plan for the area in question showing instructions for security personnel to verify doors remain secure; and
4. Training roster and training materials.

CIP-006-3c R6 (SERC2012009109)

URE's Mitigation Plan to address its violation of CIP-006-3c R6 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT006623-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. confiscate the badge and revoke access for vendor-provided custodial personnel at the facility in question;
2. conduct an internal investigation;
3. issue interim process for granting access outside normal business hours;
4. transition cleaning services to internal personnel;
5. review and update procedures for granting access to PSPs outside normal business hours; and
6. retrain individuals responsible for managing and controlling access to PSPs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. access group "action history" for revoking access for the vendor provided custodial personnel;
2. documentation of internal investigation by URE personnel;
3. copy of interim process for operation center access after normal business hours and copy of email transmittals;
4. emails documenting transitioning to URE personnel for cleaning of the operating center;

5. training roster documenting retraining of operating center personnel on revised criteria and processes; and
6. copy of updated revised criteria for granting access after normal hours.

CIP-007-1 R1 (SERC201000678)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005279-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create and implement a technical procedure requiring the necessary testing; and
2. install an operating system to monitor for changes to security controls in ESPs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Cyber Asset Test Plan along with evidence of review;
2. change tickets requesting authorization and implementation of a security and data integrity tool used for monitoring and alerting on specific file change(s) on a range of systems;
3. evidence of the data tool contract;
4. evidence of the data tool network modifications;
5. work order for hardware associated with the data tool implementation;
6. change ticket for solution testing and production rollout evidence;
7. project completion and closeout documentation; and
8. copy of testing process in place.

CIP-007-1 R2 (SERC201000734)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010426 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a technical practice document providing guidance when significant changes and security changes are performed;
2. implement a data tool to detect changes to Cyber Assets for security, document, and store all approved ports and services within the data tool;
3. implement a script to detect authorized/unauthorized ports detection in the data tool and alert support personnel of any changes, implement command on Cyber Assets for port number, port name, and executable, and verify the information in the file for approved ports and services;
4. add additional technical practice governance in business unit's procedure, Cyber Asset test plan, regarding evaluation for ports and services;
5. verify vendor or entity documentation that specific port or service is required for normal and emergency operations and disable; and
6. project closeout and implement annual reviews as part of the CVA to prevent future recurrence.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. a Cyber Asset test plan procedure document;
2. a copy of change ticket detailing the data tool project;
3. an excerpt from SCADA workstation ports list;
4. a copy of change ticket detailing implementation of the script;
5. a copy of change ticket detailing activities for implementation of commands on Critical Asset devices for port name, and executable and verify;
6. a technical practice document showing additions to the document in the title page and revision log;
7. a copy of the revision log for a procedure showing addition to the procedure plus an example of change control documentation when action is required; and
8. a procedure revision log showing additions and change ticket closed.

CIP-007-1 R3 (SERC201000735)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010423 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. eliminate legacy assets and remove difficult-to-patch legacy servers from ESP;
2. revise the patch management program and update procedure addressing enhancements to security patch evaluation and rating process to facilitate compliance;
3. revise hydro operations and facility's procedures to align with URE patch management program;
4. deploy updated procedures to those involved with the patch management program;
5. assess missing patches by reviewing vulnerability scan reports on relevant assets;
6. obtain relevant patches from proper sources and perform security testing covering each patch before deployment to production assets; and
7. coordinate outages with plant/facility management to schedule appropriate times for asset outages and install patches on production assets, pending successful security testing.

CIP-007-3a R3 (SERC2012010883)

URE's Mitigation Plan to address its violation of CIP-007-3a R3 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008191-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a formal work instruction to address adding new administrators; and
2. apply the missed security patches missed to the applicable Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. formal work instruction; and
2. screen shots illustrating application of the three security patches.

CIP-007-1 R4 (SERC201000566)

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005276 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace the existing server hardware and completed all necessary configurations enabling the new server to run malware prevention tools, as required;
2. configure the application to replace the archive server and cluster configuration to provide failover support;
3. install management tools once the operating system and cluster software was configured;
4. configure the system with the IP and hostname resources from the archive server to facilitate minimal downtime; and
5. power off and remove from network the old archive server once the cutover was complete.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the appropriate change request and change tickets from the change management process.

CIP-007-1 R4; R4.2 (SERC201000736)

URE's Mitigation Plan to address its violation of CIP-007-1 R4; R4.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010421 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform project scoping;

2. develop implementation schedule for testing malware signature files;
3. configure solution for testing malware signature files;
4. complete implementation of testing process;
5. develop work instruction or procedure detailing testing of malware signature files; and
6. train applicable staff on the testing process.

CIP-007-1 R5 (SERC201000570)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005274-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove local accounts;
2. modify the quarterly review process to include review of local accounts in addition to centralized accounts;
3. implement quarterly reviews of accounts including at least two reviewers;
4. implement a monitoring and reporting system to report configuration changes;
5. document all account changes relating to personnel with access to CCAs using the change management process;
6. change passwords for default accounts as required;
7. configure monitoring system to generate a daily password age report and alert personnel of passwords older than 300 days and implement other technical controls to ensure passwords are changed;
8. implement a system integrity monitoring solution to monitor assets to verify the integrity of cyber security posture;
9. research potential pluggable authentication module configurations with support of system vendors;
10. test the solution per change management process;
11. rollout the production of the solution per change management process;

12. document the solution per the change management process;
13. create automated alerts on passwords that are older than 330 days with the data tool reports;
14. issue a change request ticket to change passwords when it is older than 330 days;
15. create electronic calendar notification alert when a password reaches 330 days for Cyber Assets that do not report to automated monitoring and alerting system;
16. review and discuss details of violations and mitigation plan with staff; and
17. configure password requirements and monitoring tools to ensure complexity parameters are implemented as required.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. change tickets for changing passwords, account removal, and the disabling of accounts;
2. spreadsheets denoting accounts;
3. emails showing evidence of removal;
4. quarterly review notice and documentation;
5. documentation showing the data tool implementation;
6. change ticket for password changes of default accounts;
7. work orders for password changes;
8. the data tool report to configure system integrity monitoring solution to monitor asset;
9. example documentation of hardware listing in data request;
10. work order for hardware changes;
11. the data tool report showing system integrity monitoring;
12. change ticket dealing activities to implement a system integrity monitoring solution
13. research of configurations;
14. documentation of solution test per change management requirements;
15. change ticket showing production rollout of solution;
16. document showing project completion;
17. documentation of project closeout from change ticket;

18. change order creating automated alerts on aging passwords;
19. email verifying automatic notification for password resets;
20. documentation showing electronic calendar notification;
21. documentation showing staff review and discussions on the details of the violation and mitigation plan;
22. work order documenting password change;
23. change order and work order detailing changes to the password enforcement parameters configuration; and
24. documentation illustrating enforcement of password complexity requirements.

CIP-007-1 R6 (SERC201000567)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005280-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Issue 1:
    - expand security event log files on the two assets to support compliance with the standard and configure the log files to be automatically archived on a weekly basis so that log data is retained;
    - replace existing server hardware with new hardware and all associated network, storage, and application installation;
    - configure the application to replace the archive server and cluster configuration to provide failover support; and
    - configure the system, cutover to the new system, and retire the old archive server and remove it from the network.
2. Issue 2:
    - research configuration options permitting strict compliance;
    - determine preferred technical solutions;

- test solutions per its change management process;
- deploy software and system modifications as needed; and
- implement the preferred technical solutions.

3. Issue 3: configure its servers to accept and monitor logs from affected Cyber Assets.
4. Issue 4: install an alternate log archive storage system in the event of a primary network monitoring outage, preventing loss of logs during outages.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the appropriate system change request and change tickets from the change management process, showing any associated procedural modifications.

CIP-007-3a R8 (SERC2012011013)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010268 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. append existing CVA to document reviews required by CIP-007-3 R8.2 and R8.3 for each Cyber Asset within the ESP; and
2. create work papers to substantiate required reviews for ports and services and default accounts for network switches and routers within the ESP.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. revised CVA procedure document showing the addition of the execution status of CIP-007 R8.2 and R8.3 for each asset in the ESP; and
2. four files demonstrating the creation of work papers to document the CIP-007 R8.2 ports and services and R8.3 default account review for network switches and routers within the ESP.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[25]
Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[26] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2014. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a two hundred fifty thousand dollar ($250,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE self-reported 17 of the violations;
2. SERC reported that URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which SERC considered a mitigating factor, as discussed above;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. SERC determined that the violations of CIP-007-1 R1 and R2 (SERC201000678 and SERC201000734) posed a serious or substantial risk to the reliability of the BPS, as discussed above;
6. URE implemented certain above and beyond compliance measures, as discussed above; and
7. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred fifty thousand dollars ($250,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[25] *See* 18 C.F.R. § 39.7(d)(4).

[26] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Andrea B. Koch* Director of Compliance and Analytics SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net John R. Twitchell* VP and Chief Program Officer SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8205 (704) 357-7914 – facsimile jtwitchell@serc1.org

Marisa A. Sifontes* General Counsel Maggie A. Sallah* Senior Counsel James M. McGrane* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 494-7778 (704) 494-7787 (704) 357-7914 – facsimile msifontes@serc1.org msallah@serc1.org jmcgrane@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Sonia Mendonça

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity,
FERC Docket No. NP14-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
WECC2013011904	CIP-004-1	R3	Medium/ Severe	$180,000
WECC2013012378	CIP-005-1	R1; R1.5	Medium/ Severe	
WECC2013012379	CIP-005-1	R2; R2.4; R2.5	Medium/ Severe	
WECC2013012437	CIP-006-1	R1; R1.8	Medium/ Severe	
WECC2013012381	CIP-007-1	R2	Medium/ Severe	
WECC2013011811	CIP-007-1	R5; R5.2.3	Medium/ Severe	
WECC2013012380	CIP-007-3a	R8	Lower/ Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-004-1 R3 (WECC2013011904)

URE submitted a Self-Report to WECC. URE reported that five employees were granted physical access to a Physical Security Perimeter (PSP) without a valid personnel risk assessment (PRA). In addition, URE granted one employee unescorted physical access to a PSP prior to having completed a PRA.

WECC determined that URE failed to ensure PRAs were conducted for six employees prior to granting them physical access to a PSP containing Critical Cyber Assets (CCAs).

WECC determined the duration of the violation to be from thirty days after access was granted for five of the six employees at issue, through when URE revoked access for those five employees, and from when unescorted physical access was granted to the sixth employee, through when URE revoked access.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the violation exposed the seven CCAs to the possibility of unauthorized access attempts. The risk was not serious or substantial because the CCAs were equipped with electronic access, logging, and monitoring controls. In addition, URE's PSP is monitored 24 hours a day, seven days a week to prevent unauthorized physical access to areas or systems. Five of the six employees in scope had NERC CIP training completed, and all six employees are still employed with URE in good standing. The subsequent PRAs for the five employees revealed no adverse findings and the sixth employee did not access a URE PSP during the six days of access to the PSP.

URE's Mitigation Plan (WECCMIT009626) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. implement a new PRA process; and
2. enhance its access controls by implementing a procedure which no longer allows dual approval rights for physical or cyber access.

URE certified that the above Mitigation Plan requirements were completed. WECC verified that URE's Mitigation Plan was complete.

CIP-005-1 R1.5 (WECC2013012378)

WECC performed a Compliance Audit of URE. WECC determined that URE failed to ensure two Cyber Assets used in the electronic access control and monitoring of Electronic Security Perimeters (ESPs) were afforded the protective measures of CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, CIP-007 R1 and R3 through R9, CIP-008, and CIP-009. Specifically, the devices at issue consisted of a firewall manager and server.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through the present.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to provide Cyber Assets the required protective measures puts such assets and ESPs at risk to be manipulated or compromised. Such information could then be used to get access to CCAs essential to the operation of the BPS and thereby potentially disrupt the operation of the BPS. The risk was not serious or substantial because the ESPs were equipped with a security incident and events management (SIEM) technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. Finally, there was no actual manipulation or compromise of the Cyber Assets at issue or the CCAs essential to the operation of the BPS.

URE's Mitigation Plan (WECCMIT010576) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. implement CIP-005 controls on the firewall manager; and
2. deploy the physical infrastructure required for a password vault.[4]

CIP-005-1 R2: R2.4 and R2.5 (WECC2013012379)

WECC performed a Compliance Audit of URE. WECC reviewed URE's processes and procedures associated with electronic access controls, and examined the configurations of all access points to the ESPs. WECC determined that URE failed to implement strong procedural or technical controls of electronic access at all access points to the ESPs. Specifically, URE's documentation failed to identify and describe the process for access requests and authorization for external interactive access into the ESP. In addition, URE's required documentation failed to identify and describe the authentication methods.

[4] The password vault manages shared accounts. Each shared account is assigned a policy and a vault. The policy sets the rules that facilitate shared password management and controls how often the password should be changed and who has access to the account. The vault is a logical container for storing passwords. Access to vaults is restricted based on who will need access to the shared accounts and passwords stored within the vaults. Accessing the vaults and the shared accounts in the vault creates the unique audit trial.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through present.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to implement and document technical and procedural controls of electronic access at all electric access points to ESPs puts such assets and ESPs at risk to be manipulated or compromised. The risk was mitigated because the ESPs were equipped with an SIEM technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. There was no manipulation or compromise of the assets within the ESPs, the ESPs themselves, or the access points.

URE's Mitigation Plan (WECCMIT010577) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. conduct a planning and coordination meeting related to URE two-factor authentication in the generation management system (GMS); and
2. deploy the physical infrastructure required for two-factor authentication.

CIP-006-1 R1.8 (WECC2013012437)

WECC performed a Compliance Audit of URE. WECC conducted site visits to visually observe and verify that all PACS are protected from unauthorized physical access. WECC determined that URE failed to provide protective measures specified in R1.8 to Cyber Assets that authorize and/ or log access to PSPs. The devices in scope are seven workstations, one server, and six door controllers that manage, log, monitor, and provision access to all of URE's PSPs. Further, URE failed to file Technical Feasibility Exceptions (TFEs) for the six door controllers that could not technically support security logging.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through present.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices were physically located within a protected facility with physical and electronic monitoring and alarming at all times. The workstations and server reside behind the corporate firewall configured to restrict, monitor, and alert upon suspected malicious activity. The six door controllers did not have the technical capability to log security events or the ability to grant

unintentional access to individuals with malicious intent. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010577) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. submit TFEs for six door controllers;
2. evaluate and develop an architectural design to ensure strong authentication for external interactive access for the PACS;
3. conduct a status meeting to ensure the project deliverables are on target; and
4. implement strong technical controls for external interactive access to the PACS by requiring the seven administrator workstations to access the PACS via Windows terminal servers for two-factor authentication.

CIP-007-1 R2 (WECC2013012381)

WECC performed a Compliance Audit of URE. WECC determined that for three years URE failed to enable only those ports and services required for normal and emergency operations for 21 CCAs, 2 non-CCAs, 8 Electronic Access Control and Monitoring Devices (EACMs), and 7 PACS assets. Further, URE failed to establish a process to ensure that only those ports and services required for normal and emergency operations are enabled.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the devices in scope (networking equipment) are used to support 100% of URE's ESPs. The risk was mitigated because the ESPs were equipped with an SIEM technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010329) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. document the baseline ports and services in compliance with CIP-007; and
2. update its procedures to ensure the baseline documents are reviewed on an annual basis.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R5.2.3 (WECC2013011811)

URE submitted a Self-Report to WECC. URE stated it did not have a policy for managing the use of some of its shared accounts. URE has controls in place for managing who has access to the accounts, but no process in place to determine who was using the shared accounts at any given time. WECC determined that URE failed to create an audit trail of the shared accounts. The devices in scope include workstations, servers, EACMs, PACS, and access points.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through present.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE has implemented account controls on all shared accounts. Specifically, URE personnel require domain level usernames and passwords in order to access the shared accounts and all shared accounts are equipped with 24 hour a day, seven day a week monitoring and logging. The URE personnel that have access to the shared accounts in scope have PRAs and CIP training. All the devices that use the shared accounts are located within a PSP where physical access is restricted by guards and special locks. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010721) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. use the vault to meet the requirements of Standard CIP-007 R5;
2. conduct a planning and coordination meeting to discuss build-out and design of the vault technology;
3. deploy the physical infrastructure required for the vault;
4. configure the network infrastructure required for the vault; and
5. test and deploy the vault and update related documentation.

CIP-007-3a R8 (WECC2013012380)

WECC performed a Compliance Audit of URE. WECC determined that URE failed to conduct an annual Cyber Vulnerability Assessment (CVA) on all Cyber Assets within an ESP. Specifically, during the calendar year, URE failed to conduct a CVA on six assets. The assets included four CCAs (GMS workstations) and two PACS devices.

WECC determined the duration of the violation to be from when URE failed to conduct its CVA, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The assets at issue were located within a single ESP that is equipped with intrusion detection systems and an SIEM technology that provides security information and events management. Traffic to and from URE's ESPs but first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards and special locks. URE did perform a CVA on the remaining Cyber Assets within the GMS domain. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010330) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets and documenting any discrepancies for remediation; and
2. conduct a CVA on all Cyber Assets pursuant to Standard CIP-007 R8.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred eighty thousand dollars ($180,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in the penalty determination;

2. URE had an internal compliance program (ICP) at the time of the violation, which WECC considered a mitigating factor;
3. URE self-reported the violation of CIP-004-1 R3, which WECC considered a mitigating factor in penalty determination;[5]
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. The violations of CIP-006 R1, CIP-007 R5, and CIP-007 R8 posed a minimal risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above. The violations of CIP-004 R3, CIP-005 R1, CIP-005 R2, and CIP-007 R2 posed a moderate risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred eighty thousand dollars ($180,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 15, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the

[5] Although URE also self-reported the violation of CIP-007-1 R5, URE submitted the Self-Report during the Self-Certification period, and therefore WECC did not apply self-reporting credit for that violation.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

underlying facts and circumstances of the violations at issue. In reaching this determination, the NERC BOTCC also considered the factors above that WECC considered.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 801-883-6853 (801) 582-3918 – facsimile jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz

Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz Chris Luras* Director of Compliance Risk Analysis and Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entities
FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3 (URE3), Unidentified Registered Entity 4 (URE4), Unidentified Registered Entity 5 (URE5), Unidentified Registered Entity 6 (URE6) and Unidentified Registered Entity 7 (URE7) (collectively, the Unidentified Registered Entities), NERC Registry IDs# NCRXXXXX1, NCRXXXXX2, NCRXXXXX3, NCRXXXXX4, NCRXXXXX5, NCRXXXXX6, and NCRXXXXX7, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

The Unidentified Registered Entities are URE Parent Company Corp. (URE Parent Company) affiliated registered entities.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and the Unidentified Registered Entities have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the thirty-five violations[3] of CIP-003, CIP-004, CIP-005, CIP-007, and CIP-009. According to the Settlement Agreement, the Unidentified Registered Entities neither admit nor deny the violations, but have agreed to the assessed penalty of $50,000, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. The violations identified as NERC Violation Tracking Identification Numbers RFC2012010385, RFC2012010386, RFC2012010387, RFC2012010389, RFC2012010995, RFC2012011061, RFC2012011062, RFC2012011063, RFC2012011064, RFC2012011065, RFC2012011066, RFC2012011067, RFC2012011068, RFC2012011069, RFC2012011070, RFC2012011071, RFC2012011072, RFC2012011073, RFC2012011074, RFC2012011075, RFC2012011076, RFC2012011077, RFC2012011078, RFC2012011099, RFC2012011101, RFC2012011102, RFC2012011123, RFC2012011265, RFC2012011268, RFC2012011270, RFC2012011272, RFC2012011273, RFC2012011443, RFC2012011444, and RFC2012011471 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed by and between ReliabilityFirst and the Unidentified Registered Entities. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty
RFC2012011444	CIP-003-2	R6	Lower/Severe	URE1	$50,000

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty
RFC2012011471	CIP-004-1	R2; R2.1; R2.3	Lower/ Severe	URE6	$50,000
RFC2012010995				URE4	
RFC2012010385	CIP-004-3	R4; R4.2	Lower/ Moderate	URE4	
RFC2012011443				URE3	
RFC2012011272	CIP-005-3a	R1; R1.5	Medium/ Severe	URE7	
RFC2012011061	CIP-005-3	R2; R2.1; R2.2	Medium/ Severe	URE4	
RFC2012011067				URE5	
RFC2012011123				URE1	
RFC2012011071				URE6	
RFC2012011273	CIP-005-3a	R3; R3.2	Medium/ Severe	URE7	
RFC2012011078	CIP-005-1	R5; R5.2	Lower/ Severe	URE1	
RFC2012011062				URE4	
RFC2012011068				URE5	
RFC2012011072				URE6	
RFC2012010389	CIP-007-3a	R1; R1.1	Medium/ Severe	URE1	
RFC2012011063	CIP-007-1	R1; R1.3	Lower/ Severe	URE4	
RFC2012011069				URE5	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Registered Entity	Total Penalty
RFC2012011073	CIP-007-1	R1; R1.3	Lower/ Severe	URE6	$50,000
RFC2012011099				URE1	
RFC2012011101	CIP-007-1	R5	Lower/ Severe	URE1	
RFC2012011064				URE4	
RFC2012011074				URE6	
RFC2012011066				URE5	
RFC2012010386	CIP-007-1	R5; R5.3.3	Lower/ Severe	URE2	
RFC2012011077	CIP-007-3a	R5; R5.3.3	Medium/ Severe	URE7	
RFC2012011102	CIP-007-1	R6	Lower/ Severe	URE1	
RFC2012011065				URE4	
RFC2012011070				URE5	
RFC2012011075				URE6	
RFC2012010387	CIP-007-1	R6	Lower/ Severe	URE2	
RFC2012011076	CIP-007-3a	R7; R7.3	Lower/ Severe	URE6	
RFC2012011265	CIP-009-1	R1	Medium/ Severe	URE4	
RFC2012011268				URE5	
RFC2012011270				URE6	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

Compliance Background

Since the Unidentified Registered Entities' initial compliance date, the seven entities have instituted a model to assign categories of assets to particular URE Parent Company registered entities to gain efficiencies across the organization. Under this model, each shared asset type is assigned to only one registered entity so that a single registered entity retains responsibility for Critical Infrastructure Protection (CIP) compliance of that asset type.

ReliabilityFirst conducted a Compliance Audit (the Compliance Audit). The Settlement Agreement included in this Notice of Penalty resolves violations that were self-reported prior to the Compliance Audit and violations that were discovered during the Compliance Audit.

As a result of the URE Parent Company designation of assigned responsibilities of shared assets, compliance assessments of CIP-006 R2, R4, R5, R6, R7, and R8 were deferred until the subsequent CIP Compliance Audit, which included all URE Parent Company registered entities.[4]

CIP-003-2 R6 (RFC2012011444)

URE1 submitted a Self-Report stating that it was in violation of CIP-003-2 R6. URE1 discovered that it had not identified, controlled, and documented multiple completed software configuration changes on its dial-up service devices pursuant to the URE Parent Company Information Technology (IT) change control process. These devices are dial-up accessible communication processors that provide communication, time synchronization, and data handling capability. Data passes through the communication processor database and it can be retrieved remotely.

ReliabilityFirst determined that URE1 had a violation of CIP-003-2 R6 because it failed to identify, control, and document multiple completed software configuration changes on its devices.

ReliabilityFirst determined the duration of the violation to be from the date URE1 did not identify, control or document the configuration changes, through the date URE1 decommissioned the devices.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE1 did not have a systemic problem with configuration management. Due to human error, URE1 experienced an isolated occurrence of failure to follow its

[4] Possible Violations discovered during the CIP Compliance Audit will be addressed separately in the future.

documented change control and configuration management process. Although URE1 did not follow its change management process, it performed configuration testing at the time of the multiple software configuration changes to verify adequate and accurate data communication. The testing reduced the risk by validating that the devices were properly communicating to relays after the software configuration changes were implemented. The software configuration changes at issue were part of an engineering field package that required URE1 to perform multiple changes. URE1 performed the changes but did not follow its change control process when making the changes.

URE1's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating that it had been completed. URE1's Mitigation Plan required URE1 to decommission the devices at issue.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-004-1 R2.1and R2.3 (RFC2012011471 and RFC2012010995)

During the Compliance Audit, ReliabilityFirst determined that URE4 and URE6 did not conduct CIP training for multiple individuals prior to granting the individuals physical access to Critical Cyber Assets (CCAs). In addition, URE4 did not perform annual CIP training for one individual.

ReliabilityFirst determined that URE4 and URE6 each had a violation of CIP-004-1 R2.1 and R2.3 because they did not conduct CIP training for multiple individuals prior to granting the individuals physical access to CCAs, and because they did not perform annual CIP training for one individual.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE4 and URE6, through the date URE4 and URE6 completed CIP training for the individuals at issue.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The individuals at issue received non-NERC cyber awareness training, which covered similar subject matter. URE4 and URE6 had conducted a personnel risk assessment (PRA) for the individuals at issue prior to granting the individuals physical access to CCAs. URE4 and URE6 discovered nothing in the PRAs that would have disqualified the individuals from being granted physical access to CCAs.

URE6's Mitigation Plan to address the violations of URE6 and URE4 was submitted to ReliabilityFirst stating it had been completed.

URE6's Mitigation Plan required URE6 to:

1. ensure individuals are trained when required;
2. accurately record training documentation; and
3. maintain sufficient records using its database.

URE6 certified on that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE6's Mitigation Plan was complete.

In addition, ReliabilityFirst determined the mitigating activities included in URE1's Mitigation Plan addressing prior violations of CIP-004-1 R1 and R2 sufficiently mitigate URE4's and URE6's instant violations of CIP-004-1 R2.1 and R2.3. URE1's Mitigation Plan laid out milestones to implement a database, which created an automated catalogue of user access to CCAs. This catalogue was integrated with other tracking systems to provide accurate dates related to training and PRAs. The instant violations of CIP-004-1 R2, before URE Parent Company incorporated the database into its practices at URE1, URE4, and URE6.

CIP-004-3 R4.2 (RFC2012010385 and RFC2012011443)

URE4 submitted a Self-Certification to ReliabilityFirst stating that it was in violation of CIP-004-3 R4. URE4 discovered that multiple non-URE Parent Company workers at a non-URE Parent Company facility that contained a URE4 physical security perimeter (PSP) did not have their physical access rights revoked within seven calendar days of those individuals' no longer requiring access to the PSP. URE4 determined that non-Unidentified Registered Entities' personnel were not consistently notifying URE4 when their personnel no longer required physical access to URE4's PSP.

URE3 submitted a Self-Report stating that it was in violation of CIP-004-3 R4.2. URE3 did not revoke physical access within seven calendar days for an administrative assistant who no longer required physical access.

ReliabilityFirst determined that URE4 and URE3 each had a violation of CIP-004-3 R4.3 because they did not revoke physical access to CCAs within seven calendar days for several individuals who no longer required physical access.

ReliabilityFirst determined the duration of the violation for URE4 to be from the date by which the workers should have had their physical access revoked, through the date their access was revoked.

The duration of the violation for URE3 was from the date URE3 should have revoked the administrative assistant's access, through the date access was revoked.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. None of the individuals at issue was terminated for cause, and none had logical access to URE Parent Company's CCAs. All individuals at issue had CIP training and PRAs at the time the violation occurred. Additionally, none of the individuals at issue accessed URE Parent Company's CCAs after it was determined that they no longer required access.

URE4's Mitigation Plan to address its violation of CIP-004-3 R4.2 was submitted to ReliabilityFirst stating it had been completed.

URE4's Mitigation Plan required URE4 to:

1. revoke access for the workers at issue; and
2. establish a process to notify URE4 when personnel with access to its PSP are transferred or no longer require PSP access.

URE4 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE4's Mitigation Plan was complete.

ReliabilityFirst determined that URE3's violation did not require a formal Mitigation Plan. URE3 revoked the access of the administrative assistant at issue. URE3 submitted evidence that it had revoked the access. ReliabilityFirst verified that URE3 completed the necessary mitigating activities.

CIP-005-3a R1.5 (RFC2012011272)

During the Compliance Audit, ReliabilityFirst determined that URE7 was using an administrator account on a checkpoint firewall that was not removed, disabled, or renamed as required by CIP-007-3 R5.2.1, referenced in CIP-005-3 R1.5. ReliabilityFirst determined that URE7 did not change the account name before the firewall went into service.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE7, through the date URE7 changed the password on the account.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, default account information on a firewall could leave

Unidentified Registered Entities' systems vulnerable to potential compromise. Default account information may be available in vendor publications, books, or on the internet and could be exploited by a malicious actor, thereby putting Unidentified Registered Entities' systems at a higher risk than those protected by non-default account information. The risk was mitigated by the fact that URE Parent Company employs a system of layered defenses. This defense-in-depth strategy provides additional layers of defense against unauthorized access and thereby mitigates the risk posed by the violation.

URE7's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE7's Mitigation Plan required URE7 to change the local default administrator account name for the checkpoint firewall.

In addition to the actions required by the Mitigation Plan, URE Parent Company affiliates, including URE7, combined their individual CIP programs into a single consolidated URE Parent Company CIP Program. As part of this consolidation, URE Parent Company developed more robust processes and procedures to ensure that accounts are removed, disabled, or renamed pursuant to CIP-007 R5.2.1 and CIP-005-3 R1.5. These processes and procedures included a change control and configuration management process that, among other things, ensures generic account names are changed before placing devices into service.

URE7 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE7's Mitigation Plan was complete.

CIP-005-3 R2.1 and R2.2 (RFC2012011061, RFC2012011067, RFC2012011123, and RFC2012011071)

URE4, URE5, and URE6 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-005-3 R2.1 and R2.2. URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of the same Reliability Standard and Requirements. URE4, URE5, URE6, and URE1 discovered that a network redesign (Redesign), which terminated some of their access control devices on a different cluster of firewalls, resulted in these devices not fully implementing the requirements of CIP-005-3 R2.1 and R2.2. Following the Redesign, the devices no longer denied access by default and did not independently restrict access to the associated ESP.

ReliabilityFirst determined that URE4, URE5, URE6, and URE1 had a violation of CIP-005-3 R2.1 and R2.2 because they did not enable their respective devices at issue to deny access by default and did not independently restrict access to the associated ESP.

ReliabilityFirst determined the duration of the violations to be from the date URE4, URE5, URE6 and URE1 performed the Redesign, through the date they configured the devices to deny all electronic communication transactions within the facility wide area network.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1, URE4, URE5, and URE6 had access control at the devices, access control via the upstream firewall, and access control to individual devices via server authentication. Furthermore, URE1, URE4, URE5, and URE6 had layered intrusion prevention defenses. These defenses included firewalls, intrusion detection and prevention defenses, malicious software prevention, and encryption, thereby limiting the risk from, and exposure to, external threats.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst on stating they had been completed.

The Mitigation Plans required the entities to:

1. configure the access control lists on the devices to deny all electronic communication transactions within the facility network; and

2. configure the devices to restrict specific point access to the ESP and deny all other access to the ESP by default.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plans requirements were completed.

ReliabilityFirst verified that URE1, URE4, URE5, and URE6's Mitigation Plans were complete.

CIP-005-3a R3.2 (RFC2012011273)

During the Compliance Audit, ReliabilityFirst determined that URE7 was in violation of CIP-005-3a R3.2. URE7 did not adequately alert for access attempts or actual unauthorized access to its ESP. URE7 only alerted for failed login and local account creation for the duration of the violation.

ReliabilityFirst determined that URE7 had a violation of CIP-005-3a R3.2 because it did not implement a security monitoring process that detects and alerts for attempts at or actual unauthorized accesses.

ReliabilityFirst determined the duration of the violation to be from the date URE7 implemented a process which did not require URE7 to detect or alert for attempted or actual unauthorized access to its ESP, through the date URE7 revised its security monitoring process to detect and alert for attempted or actual unauthorized access to its ESP.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE7 continuously monitors and logs system events on the Cyber Assets within the ESP, as required by CIP-007 R6. URE7's firewalls were functioning properly by filtering and denying unauthorized access attempts to the ESP for the duration of the violation. URE7's firewalls were denying unauthorized access attempts to the ESP. URE7 did not receive alerts regarding unauthorized access attempts.

URE7's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE7's Mitigation Plan required URE7 to establish a security monitoring procedure that detects and alerts for access attempts to the ESP. The procedure requires logs of user account activity as required by CIP-007-3 R5.1.2.

URE7 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE7's Mitigation Plan was complete.

CIP-005-1 R5.2 (RFC2012011062, RFC2012011068, RFC2012011072 and RFC2012011078)

URE1, URE4, URE5, and URE6 each submitted a Self-Report to ReliabilityFirst stating that they were in violation of CIP-005-1 R5. URE1, URE4, URE5, and URE6 discovered that each of them had failed to document changes to their ESP drawing resulting from the Redesign.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-005-1 R5.2 because they did not document within 90 days a modification that resulted in some of their respective devices terminating on a different cluster of firewalls.

ReliabilityFirst determined the duration of these violations to be from the date the entities should have documented the changes to the ESP, through the date the entities updated the ESP drawings to reflect the changes resulting from the Redesign.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations consisted of documentation errors. Specifically, although the drawings were not updated within 90 days to reflect the change to the network, appropriate URE Parent Company personnel prepared, approved, and implemented the changes. Further, all appropriate personnel were aware of the change because of the limited number of electronic access points and the fact that a small team of people maintains those assets.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst, stating the four Mitigation Plans had been completed.

The Mitigation Plans required the entities to update their ESP drawings at issue to reflect the Redesign changes.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plans requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-3a R1.1 (RFC2012010389)

URE1 submitted a Self-Certification to ReliabilityFirst stating that it was in violation of CIP-007-3a R1. URE1 determined that it prematurely installed an operating system security patch on multiple CCAs before the patch had been fully tested in accordance with URE1's cybersecurity test procedures. Specifically, URE1 determined that it had not tested the security patch in a CIP test environment to determine if the installation would result in any adverse effects to existing cybersecurity controls.

ReliabilityFirst determined that URE1 had a violation of CIP-007-3a R1.1 because it installed a system security patch on multiple CCAs before testing the patch.

ReliabilityFirst determined the duration of the violation to be from the date URE1 installed the security patch on the CCAs at issue, through the date URE1 tested the security patch in accordance with its cybersecurity test procedures.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The duration of the violation was short. URE1 quickly identified the issue and performed the required testing within a week. All patches were approved by third-party vendors. Additionally, upon testing the security patch in accordance with its cybersecurity test procedures, URE1 determined that the patch had no compatibility issues with the CCAs or their associated applications. The CCAs at issue were not needed or used for the duration of the violation. Therefore,

the security patch had no adverse effects on the existing cybersecurity controls for the duration of the violation.

URE1 memorialized the actions it took to address this violation and no formal Mitigation Plan was required. URE1 tested the security patch at issue in accordance with its cybersecurity test procedures. Additionally, URE1 reconfigured software on applicable CIP workstations to ensure that patches are only available to those CIP workstations after IT real-time operations testers have tested and approved the security patches.

URE1 submitted evidence that it completed the mitigating activities.

ReliabilityFirst verified that URE1 completed the mitigating activities.

CIP-007-1 R1.3 (RFC2012011063, RFC2012011069, RFC2012011073, and RFC2012011099)

URE4, URE5, and URE6 each submitted a Self-Report stating that they were in violation of CIP-007-3 R1.3. URE1 submitted a Self-Report stating that it was in violation of CIP-007-1 R1.3. URE1, URE4, URE5, and URE6 discovered that they had not adequately documented the testing each entity performed on some of their devices to ensure these devices did not adversely affect existing cybersecurity controls.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-007-3 R1.3 because they did not document the test results for their devices.

ReliabilityFirst determined the duration of these violations to be from the date on which URE1, URE4, URE5, and URE6 were required to comply with this Standard, through the date they disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1, URE4, URE5, and URE6 performed testing required by CIP-007-1 R1 on the dial-up devices in accordance with URE Parent Company's approved test procedures; these violations represented documentation errors. Additionally, for the duration of the violations, URE1, URE4, URE5, and URE6 had implemented automated tools and organizational process controls to monitor events related to cybersecurity for remote access to the devices.

URE1, URE4, URE5, and URE6's Mitigation to address these violations were submitted to ReliabilityFirst on stating they had been completed.

URE1, URE4, URE5, and URE6's Mitigation Plan required the entities to disconnect the dial-up connections and decommission the devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-1 R5 (RFC2012011101, RFC2012011064, RFC2012011074, and RFC2012011066)

URE1, URE4, URE5, and URE6 each submitted a Self-Report to ReliabilityFirst stating that they were in violation of CIP-007-1 R5. URE1, URE4, URE5, and URE6 discovered that they had not established, implemented, and documented technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access to a single local access port on some of their respective devices. URE1, URE4, URE5, and URE6 established, implemented, and documented remote access processes to ensure compliance with CIP-007-1 R5, but had not extended those processes to the local access port.

ReliabilityFirst determined that URE1, URE4, URE5, and URE6 each had a violation of CIP-007-1 R5 because they did not establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all local logical access to dial-up devices.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1, URE4, URE5, and URE6, through the date they disconnected dial-up connections and decommissioned the devices at issue.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Unauthorized access to the local service port on the devices would require physical access through a locked fence and a locked building door, which is monitored for entry by URE Parent Company. Access via the local service port is password-protected, and an alarm is generated the event of unauthorized access attempts to the devices. Finally, for remote access to the devices at issue, URE1, URE4, URE5, and URE6 implemented automated tools and organizational process controls to monitor system events that are related to cybersecurity.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst, stating the Mitigation Plans had been completed.

URE1, URE4, URE5, and URE6's Mitigation Plans required them to disconnect dial-up connections and decommission the devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were complete.

ReliabilityFirst verified that URE1, URE4, URE5, and URE6's Mitigation Plans were complete.

CIP-007-1 R5.3.3 (RFC2012010386)

On May 2, 2012, URE2 submitted a Self-Certification stating that it was in violation of CIP-007-1 R5.3.3. During its Cyber Vulnerability Assessment, URE2 determined that it did not annually change passwords for multiple local accounts at one Critical Asset facility, and that it did not delete these accounts when it installed an active directory to manage passwords. Additionally, URE2 determined it did not establish log-on passwords for the shared operator account on several devices at the same facility.

ReliabilityFirst determined that URE2 had a violation of CIP-007-1 R5.3.3 for a failure to change passwords annually for one Critical Asset facility.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2, through the date URE2 decommissioned the applicable Critical Asset.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices at issue were located within a PSP. URE2 employs a system of layered defenses. This defense-in-depth strategy provides additional layers of defense against unauthorized access and reduces the risk posed by this violation.

URE2's Mitigation Plan to address this violation was submitted to ReliabilityFirst, stating it had been completed.

URE2's Mitigation Plan required URE2 to disable the local accounts and to decommission the Cyber Assets at issue.

URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R5.3.3 (RFC2012011077)

URE7 submitted a Self-Report stating that it was in violation of CIP-007-3a R5.3.3. URE7 discovered that it had not updated passwords for multiple individual user accounts and several shared system accounts annually. Prior to the discovery of this violation, the CCAs at issues were migrated from a legacy CIP program to a new URE Parent Company CIP program, which included affiliated companies. Because of the consolidation of programs, the timing of the controls occurred such that annual password changes for the passwords at issue occurred more than 15 months apart when these password changes were synchronized with the combined URE Parent Company CIP program.

ReliabilityFirst determined that URE7 had a violation of CIP-007-3a R5.3.3 for its failure to change passwords annually for several accounts.

ReliabilityFirst determined the duration of the violation to be from the date by which URE7 should have updated its passwords, through the date URE7 updated the passwords at issue.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The duration of the violation was approximately one month. Furthermore, the passwords addressed the complexity requirements of CIP-007-3a R.5.3.1 and R5.3.2. Finally, the passwords at issue were available to authorized users only.

ReliabilityFirst determined that a formal Mitigation Plan was not required for this violation. In its Self-Report, URE7 represented that it completed all necessary mitigating actions to address this violation. URE7 changed all passwords at issue. Further, URE Parent Company's CIP program, which URE7 now follows, requires that the dates of the last password change be reviewed every six months, thus reducing the likelihood of missing an annual update.

URE7 submitted evidence that it completed these mitigating activities. ReliabilityFirst verified completion of these mitigating activities.

CIP-007-1 R6 (RFC2012011102, RFC2012011065, RFC2012011070, and RFC2012011075)

URE1, URE4, URE5, and URE6 each submitted a Self-Report stating that each was in violation of CIP-007-1 R6. URE1, URE4, URE5, and URE6 discovered that they had not adequately monitored local logical access to some devices for system events that are related to cybersecurity.

ReliabilityFirst determined that URE1, URE4, URE5 and URE6 each had a violation of CIP-007-1 R6 for a failure to monitor system events related to cybersecurity of some of their devices.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1, URE4, URE5, and URE6, through the date the entities disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Unauthorized access to the local service port on the devices would require physical access through a locked fence and a locked door which is monitored for entry. Access via the local service port is password-protected, and an alarm is generated in the URE Parent Company in the event of unauthorized access attempts the devices. Finally, for remote access to the devices, URE1, URE4, URE5, and URE6 implemented automated tools and organizational process controls to monitor system events that are related to cybersecurity.

URE1, URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst stating they had been completed.

URE1, URE4, URE5, and URE6's Mitigation Plans required these entities to disconnect dial-up connections and decommission the dial-up devices at issue.

URE1, URE4, URE5, and URE6 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE1, URE4, URE5, and URE6 Mitigation Plans were complete.

CIP-007-1 R6 (RFC2012010387)

URE2 submitted a Self-Certification stating that it was in violation of CIP-007-1 R6. URE2 discovered that it had not adequately implemented organizational processes and technical and procedural mechanisms for monitoring security events for several CCAs. URE2 discovered this violation after it decommissioned the CCAs at issue.

ReliabilityFirst determined that URE2 had a violation of CIP-007-1 R6 for failing to implement adequately organizational processes and technical and procedural mechanisms for monitoring security events on several CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE2, through the date URE2 decommissioned the CCAs at issue.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, use of the network switches by a malicious actor could result in the loss of operational control or visibility. Further, without security controls and monitoring in place, the malicious actor could remain undetected. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. These CCAs were enclosed in PSPs during the violation period, and physical access was controlled and monitored in accordance with the CIP Standards. Further, during the violation period, access points to the ESPs and other CIP Cyber Assets in the ESPs were monitored, and logging was performed as required by the CIP Standards.

URE2's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to decommission the CCAs at issue.

URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R7.3 (RFC2012011076)

URE6 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3 R7.3. When one URE6 device failed in service, URE6 sent the device for repair. Upon receipt of the repaired device, URE6 designated the device as a spare device and placed it in storage. URE6 did not properly maintain records associated with the redeployment of the device. Upon decommissioning of the device, URE6 discovered that it did not maintain redeployment records after it removed the device from service for repair.

ReliabilityFirst determined that URE6 had a violation of CIP-007-3 R7.3 for its failure to maintain records that it redeployed one device in accordance with its documented procedures.

ReliabilityFirst determined the duration of the violation to be from the date URE6 redeployed the single device as a spare device, through the date URE6 disconnected dial-up connections and decommissioned the device.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. ReliabilityFirst determined that this violation involved a documentation issue because URE6 redeployed the device pursuant to CIP-007 R7, but it did not maintain the associated records adequately.

URE6's Mitigation Plan to address this violation was submitted to ReliabilityFirst, stating that it had been completed.

URE6's Mitigation Plan required URE6 to disconnect the dial-up connections and decommission the device at issue.

URE6 certified that the above Mitigation Plan requirements were completed.

On August 5, 2013, ReliabilityFirst verified that URE6's Mitigation Plan was complete.

CIP-009-1 R1 (RFC2012011265, RFC2012011268, and RFC2012011270)

During the Compliance Audit, ReliabilityFirst determined that URE4, URE5, and URE6 did not have an adequate recovery plan for some of their respective devices. URE4, URE5, and URE6 had procedures to address recovery of the devices at issue. However, these procedures did not address all the elements required by CIP-009-1 R1. The applicable procedures did not specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan and did not define the roles and responsibilities of responders.

ReliabilityFirst determined that URE4, URE5, and URE6 each had a violation of CIP-009-3 R1 because they did not have adequate recovery plans for their respective devices.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE4, URE5, and URE6, through the date the entities disconnected the dial-up connections and decommissioned the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The recovery plans identified other procedures that were invoked by the loss of a communication processor and the overall steps to address repair or replacement of the devices in

the event of a communication processor failure. In addition, the recovery plan did identify the responders, although it did not adequately define the roles and responsibilities of those responders. Further, the violation did not indicate a systemic issue with URE4, URE5, and URE6's respective recovery plans. During the Compliance Audit, ReliabilityFirst determined these Unidentified Registered Entities had recovery plans for all devices except the devices.

URE4, URE5, and URE6's Mitigation Plans to address these violations were submitted to ReliabilityFirst stating they had been completed.

URE4, URE5, and URE6's Mitigation Plans required the entities to disconnect the dial-up connections and decommission the devices.

URE4, URE5, and URE6 certified on that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE4, URE5, and URE6's Mitigation Plans were complete.

Internal Control Improvements

ReliabilityFirst determined that the Unidentified Registered Entities have implemented programs and procedures that substantially improve their shared compliance program by optimizing the Unidentified Registered Entities' operations and security. Many of these improvements began as part of an effort to consolidate the Unidentified Registered Entities' separate compliance programs into a single compliance program. Many of the instant violations were corrected in the scope of the Unidentified Registered Entities' efforts, and therefore represent historical compliance issues. Unidentified Registered Entities' efforts to improve compliance had affected five major compliance areas: 1) change control and configuration management; 2) cybersecurity logging; 3) identifying and classifying Cyber Assets; 4) access control and account management; and 5) testing.

Thus, ReliabilityFirst determined that the internal controls improvements outlined above, which can be tied to the key management practices of asset and configuration management and reliability quality management, have positioned URE Parent Company to be more reliable and compliant on a going-forward basis.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of fifty thousand dollars ($50,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. the violations constituted Unidentified Registered Entities' fifth occurrence of same or similar violations of CIP-004 and second occurrence of same or similar violations of CIP-007. ReliabilityFirst considered the compliance history of the Unidentified Registered Entities as an aggravating factor in the penalty determination, but not a substantial aggravating factor;
2. the subsequent CIP Compliance Audit findings (to be addressed separately in the future) demonstrated the Unidentified Registered Entities' maturing compliance program through its efforts to improve internal controls;
3. ReliabilityFirst awarded significant mitigating credit to recognize and incent the Unidentified Registered Entities' substantial and voluntary commitment to improve its operations and compliance program. ReliabilityFirst favorably considered the Unidentified Registered Entities' efforts, which ReliabilityFirst observed firsthand during the Compliance Audit, at improving CIP compliance and enhancing the reliability of the BPS;
4. ReliabilityFirst favorably considered certain aspects of the Unidentified Registered Entities' compliance programs. ReliabilityFirst also favorably considered the various improvements to URE Parent Company's compliance program and internal controls, which largely began prior to the Compliance Audit and address legacy issues that led to findings of noncompliance at the Compliance Audit;
5. the Unidentified Registered Entities self-reported 24 of the violations;[5]
6. of the total 35 violations, 33 violations posed minimal risk to the reliability of the BPS, as discussed above. The violations did not indicate systemic failure, and were promptly mitigated;
7. two of the 35 violations posed a moderate risk to the reliability of the BPS, as discussed above;
8. the Unidentified Registered Entities were cooperative throughout the compliance enforcement process;
9. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[5] ReliabilityFirst applied partial mitigating credit for 21 of the 24 Self-Reports and full mitigating credit for the remaining three Self-Reports.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of fifty thousand dollars ($50,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 15, 2014. The NERC BOTCC approved the Settlement Agreement, including ReliabilityFirst's assessment of a fifty-thousand dollar ($50,000) financial penalty against the Unidentified Registered Entities and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by ReliabilityFirst, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of fifty thousand dollars ($50,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (216) 503-0689 (216) 503-9207 – facsimile niki.schaefer@rfirst.org	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net
L. Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542 (216) 503-0683	Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 320 Springside Drive, Suite 300 Akron, OH 44333-4542

(216) 503-9207 – facsimile jason.blake@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	(216) 503-0682 (216) 503-9207 – facsimile bob.wargo@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Director of
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entities
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

August 27, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), and Unidentified Registered Entity 3 (URE3), FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), NERC Registry ID# NCRXXXXX, Unidentified Registered Entity 2 (URE2), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 3 (URE3), NERC Registry ID# NCRXXXXX (collectively, the URE Companies) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and the URE Companies have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the URE Companies neither admit nor deny the violations, but have agreed to the assessed penalty of six hundred and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

twenty-five thousand dollars ($625,000) and the non-monetary penalty of an additional Spot Check, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement and Attachment A to the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010910	CIP-002-1	R2	High/ Severe	URE2	$625,000
RFC2012010911 NPCC2014013552	CIP-002-1	R3	High/ Severe	URE2	
RFC2012010912 NPCC2014013553	CIP-002-1	R4	Lower/ Severe	URE2	
RFC2013011925	CIP-003-1	R1; R1.3	Lower/ Severe	URE1	
RFC2014013690 NPCC2014013556				URE2	
RFC2014013691				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010093	CIP-003-1	R4	Medium/ High	URE1	$625,000
RFC2012010086				URE2	
RFC2012010079				URE3	
RFC201100889	CIP-003-1	R5	Lower/ High	URE1	
RFC201100896				URE2	
RFC201100903				URE3	
RFC2012010302 NPCC2014013554	CIP-003-1	R6	Lower/ Severe	URE2	
RFC2013011966				URE3	
RFC2012010303 NPCC2014013550	CIP-004-1	R3	Medium/ Severe	URE2	
RFC2012011364	CIP-004-3a	R3	Medium/ High	URE1	
RFC2014013316				URE3	
RFC2012010094	CIP-004-1	R4	Lower/ Severe	URE1	
RFC2012010087 NPCC2014013549				URE2	
RFC2012010080				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010924	CIP-005-1	R1	Medium/ Severe	URE1	$625,000
RFC2012010305 NPCC2014013440				URE2	
RFC2013011967				URE3	
RFC201100890	CIP-005-1	R2	Medium/ Severe	URE1	
RFC201100897 NPCC2014013551				URE2	
RFC201100904				URE3	
RFC201100891	CIP-005-1	R3	Medium/ Severe	URE1	
RFC201100898 NPCC2014013548				URE2	
RFC201100905				URE3	
RFC2012010311	CIP-005-1	R4	Medium/ Severe	URE1	
RFC2012010297 NPCC2014013541				URE2	
RFC2012010314				URE3	
RFC2012010310	CIP-005-1	R5	Lower/ Severe	URE1	
RFC2012010298 NPCC2014013534				URE2	
RFC2012010315				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC201100892	CIP-006-3c	R1	Medium/ Severe	URE1	$625,000
RFC201100899 NPCC2014013536				URE2	
RFC201100906				URE3	
RFC2014013708	CIP-006-2	R2; R2.2	Medium/ Severe	URE1	
RFC2014013709 NPCC2014013535				URE2	
RFC2014013703				URE3	
RFC201100893	CIP-006-3c	R6	Lower/ Severe	URE1	
RFC201100900				URE2	
RFC201100907				URE3	
RFC201100894	CIP-007-1	R1	Medium/ Severe	URE1	
RFC201100901 NPCC2014013546				URE2	
RFC201100908				URE3	
RFC201100895	CIP-007-1	R2	Medium/ Severe	URE1	
RFC201100902 NPCC2014013545				URE2	
RFC201100909				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010095	CIP-007-1	R3	Lower/ Severe	URE1	$625,000
RFC2012010088 NPCC2014013544				URE2	
RFC2012010081				URE3	
RFC2012010096	CIP-007-1	R4	Medium/ Severe	URE1	
RFC2012010089				URE2	
RFC2012010082				URE3	
RFC2012010097	CIP-007-1	R5	Lower/ Severe	URE1	
RFC2012010090 NPCC2014013537				URE2	
RFC2012010083				URE3	
RFC2012010098	CIP-007-1	R6	Lower/ Severe	URE1	
RFC2012010091 NPCC2014013543				URE2	
RFC2012010084				URE3	
RFC2012010925	CIP-007-1	R7	Lower/ Severe	URE1	
RFC2012010921 NPCC2014013542				URE2	
RFC2013011968				URE3	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
RFC2012010099	CIP-007-1	R8	Lower/ Severe	URE1	$625,000
RFC2012010092 NPCC2014013540				URE2	
RFC2012010085				URE3	
RFC2012010313	CIP-007-1	R9	Lower/ High	URE1	
RFC2012010301 NPCC2014013539				URE2	
RFC2012010317				URE3	
RFC2012010926	CIP-008-1	R1	Lower/ High	URE1	
RFC2012010907 NPCC2014013538				URE2	
RFC2013011970				URE3	
RFC2012010927	CIP-009-1	R1	Medium/ Severe	URE1	
RFC2012010908 NPCC2014013547				URE2	
RFC2013011971				URE3	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

BACKGROUND

The Settlement Agreement that is the subject of this Notice of Penalty resolves 100 violations covering multiple instances of noncompliance with CIP Reliability Standards. The violations were discovered through a combination of Self-Reports and findings from three Compliance Audits (one for each of the three entities). As they are all subsidiaries of the same corporation and subject to many of the same processes and procedures, many of the facts and circumstances of the violations apply to URE1, URE2, and URE3.

The full scope of these violations required longer-term, more comprehensive mitigation. ReliabilityFirst worked closely with the URE Companies, conducting an assist visit to help the URE Companies develop thorough and complete mitigation. This also helped to ensure that, in the interim, the violations posed no serious risks to the reliability of the bulk power system (BPS).

After determining the full scope of the violations and the mitigation activities, ReliabilityFirst observed that the state of the URE Companies' mitigation activities and compliance had not progressed as quickly as expected considering the time they had been working together to resolve these violations. This factor, along with the other adjustment factors set forth in the Regional Entity's Basis for Penalty section below, formed the basis of the $625,000 monetary penalty associated with this Settlement Agreement.

No harm to the BPS is known to have occurred as a result of the violations described in this Notice of Penalty.

CIP-002-1 R2 (RFC2012010910)

ReliabilityFirst conducted a Compliance Audit of URE2 (URE2 Compliance Audit). During the URE2 Compliance Audit, URE2 did not provide evidence that it performed a power flow analysis when developing its list of Critical Assets, as required by its risk-based assessment methodology.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R2 for failing to develop a list of its identified Critical Assets through an annual application of its risk-based assessment methodology.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE2 had a procedure that stated other criteria for the identification of Critical

Assets. Further, a power flow analysis is not required by CIP-002 R2 to identify Critical Assets, nor is it typically included in a registered entity's risk-based assessment methodology as a criterion for the identification of Critical Assets. URE2 mistakenly included the power flow analysis in its risk-based assessment methodology; it was intended to be a tool for third parties to confirm URE2's classification of assets.

URE2's Mitigation Plan to address this violation was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to modify its procedure to eliminate the requirement for power flow analysis.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-002-1 R3 (RFC2012010911, NPCC2014013552)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to maintain documentation to demonstrate that it evaluated all Cyber Assets associated with a Critical Asset when developing its list of Critical Cyber Assets (CCAs). URE2 represented that it performed an annual review of its CCA list, but that its evidence was incomplete in part. During the URE2 Compliance Audit, URE2 presented CCA lists that did not list an effective date or accurately reflect existing CCAs essential to the operation of the Critical Assets. In addition, URE2's documentation of annual approval of the CCA lists did not associate the approval form with a specific CCA list.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R3 for failing to develop its lists of CCAs using the lists of Critical Assets developed pursuant to Requirement R2.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE2's failure to develop complete CCA lists with dates and other necessary information increased the possibility that URE2 would not identify and afford the protections of the CIP Standards to all CCAs. However, URE2 did perform an annual review of its documentation, although it did not retain strong evidence regarding such reviews. Therefore, ReliabilityFirst considered this violation to relate to a documentation error.

URE2's Mitigation Plan to address these violations was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to implement a change to require the approver to sign and date the actual CCA list reviewed in addition to the completion of any formally-assigned workflows.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-002-1 R4 (RFC2012010912, NPCC2014013553)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to ensure that a senior manager or delegate approved the list of Critical Assets, the list of CCAs, and the risk-based assessment methodology on an annual basis. Specifically, URE2 did not provide any evidence of senior manager or delegate approval of the risk-based assessment methodology. Instead, the evidence did not indicate or identify the CCA list that the URE2 senior manager or delegate reviewed or approved. Further, URE2 did not associate its approval forms with specific Critical Asset lists. The evidence did not indicate or identify the Critical Asset list that the URE2 senior manager or delegate reviewed or approved.

ReliabilityFirst determined that URE2 had a violation of CIP-002-1 R4 for failing to ensure that a senior manager or delegate annually approve the list of Critical Assets, the list of CCAs, and the risk-based assessment methodology.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it did not retain sufficient evidence, a senior manager or delegate did in fact perform an annual review of the list of Critical Assets, list of CCAs, and risk-based assessment methodology.

URE2's Mitigation Plan to address these violations was submitted to ReliabilityFirst stating it had been completed.

URE2's Mitigation Plan required URE2 to review and implement updates to its designation and delegation documents to identify any areas for improvement and incorporate more specific delegation information into the designating document.

URE2 certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R1 (RFC2013011925, RFC2014013690, RFC2014013691, NPCC2014013556)

ReliabilityFirst conducted a Compliance Audit of URE1 (URE1 Compliance Audit). During the URE1 Compliance Audit, URE1 reported to ReliabilityFirst that the facts and circumstances described in its previously-submitted CIP-003-1 R4 Self-Report also involved a violation of CIP-003-1 R1.3. Specifically, URE1 did not ensure that the assigned senior manager conducted an annual review and approval of URE1's cybersecurity policy.

Subsequently, URE2 and URE3 submitted Self-Reports to ReliabilityFirst to the same effect.

ReliabilityFirst determined that the URE Companies had violations of CIP-003-1 R1.3 for failing to conduct an annual review and approval of the cybersecurity policy by the senior manager assigned pursuant to CIP-003 R2.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. While the URE Companies failed to retain strong evidence, the URE Companies did in fact perform annual reviews of their cybersecurity policies.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their cybersecurity policies and update the change logs;
2. enhance the documentation for annual reviews of the cybersecurity policies; and
3. use their processes to ensure completion of annual reviews.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R4 (RFC2012010079, RFC2012010086, RFC2012010093)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-003-1 R4 for failing to implement their CCA information protection programs. Specifically, the URE Companies failed to properly classify and protect information repositories that house CCA information. Additionally, the URE Companies failed to complete the annual assessments of the CCA information protection programs, document the results of such assessments, and implement remediation plans for potential issues in accordance with CIP-003-1 R4.3.

ReliabilityFirst determined that each of the URE Companies had violations of CIP-003-1 R4 for failing to implement its program to identify, classify, and protect information associated with CCAs, and for failing to assess annually adherence to its CCA information protection program, document the assessment results, and implement an action plan to remediate deficiencies.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure of the URE Companies to implement and document their programs to identify, classify, and protect information repositories that housed CCA information increased the possibility that the protections in place for protected CCA information would be decreased or eliminated.

However, the risk was mitigated by several factors. Although the URE Companies failed to classify appropriately certain files containing protected information, this information did reside in secure locations with access control mechanisms implemented. The URE Companies store their CCA information in repositories housed on their internal networks, which allow access to only those individuals housed on the URE Companies internal networks and bearing user access credentials. In most cases, shared drives and similar repositories that have department and/or team-level access restrictions housed these repositories. These access restrictions required specific approvals by a management-level official or higher in order to ensure the individuals who authorized the access were personnel in trusted supervisory roles and with requisite knowledge of the access need of the requested employee. In other instances, physical repositories (i.e., locked file cabinets) were located within an existing Physical Security Perimeter (PSP), which had physical protections and access restrictions.

Further, while the URE Companies failed to maintain adequate documentation of their annual reviews of the CCA information protection programs, the URE Companies did in fact perform these annual reviews.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their protected information to ensure it resides within a protected information repository;
2. develop revisions to their restricted information procedures and processes and train relevant staff on these revisions;
3. develop and implement a plan to assure proper classification in the first instance to minimize possibility of over classification of protected information; and
4. implement their annual reviews of their information protection programs.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R5 (RFC201100889, RFC201100896, RFC201100903)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they failed to implement their program for managing vendor access to protected CCA information. Specifically, the URE Companies did not verify that the external vendor personnel who could access protected CCA information during the course of their IT support functions met the requirements for training and personnel risk assessments (PRAs) prior to granting access to such information.

The URE Companies subsequently reported that they failed to classify properly information repositories that housed CCA information and subsequently failed to provide the repositories and the information within the repositories with the protections specified within their program for managing access to protected CCA information. URE2 properly classified its two repositories, but stored information that was not properly classified in those repositories. URE1 under-classified approximately 15% of its repositories, and URE3 under-classified approximately 25% of its repositories.

During the URE2 Compliance Audit, URE2 failed to provide evidence of an annual verification of personnel responsible for authorizing access to protected information or an annual review of the

access privileges to protected information to confirm that access privileges are correct and correspond with URE2's needs and appropriate personnel roles and responsibilities.

In addition, the URE Companies reported that they did not retain evidence of grandfathered users' need for access for a number of individuals with access to protected information. Therefore, the URE Companies failed to document that their access privileges were correct and that they corresponded with the URE Companies' needs and appropriate roles and responsibilities.

ReliabilityFirst determined that the URE Companies had violations of CIP-003-1 R5 for failing to implement their program for managing access to protected CCA information.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to implement their program for managing access to protected CCA information increased the possibility that protections in place for access to protected CCA information would be decreased.

However, ReliabilityFirst determined that the URE Companies implemented certain controls to provide security to their Critical Assets and CCAs. First, although the URE Companies failed to classify appropriately certain files containing protected information and provide the information with the protections specified in their programs, this information did reside in secure locations with access control mechanisms implemented. See the risk assessment for CIP-003-1 R4 (RFC2012010079, RFC2012010086, RFC2012010093) above. Second, the URE Companies subsequently verified that the external vendor personnel with access to protected CCA information completed the training and PRA requirements.

Third, the individuals without confirmed access privileges were initially granted access during their work on the NERC CIP compliance development team, which occurred prior to the mandatory and enforceable date of the Standard. Although the URE Companies' documentation was insufficient, all of these individuals were and are trusted users who have approved network access credentials.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The URE Companies' Mitigation Plans required the URE Companies to:

1. review their protected information to ensure that it resides within a protected information repository;
2. develop and communicate revisions to their restricted information policies and procedures;
3. review user PRA records, training records, access control lists, and user access privileges to protected information; and
4. review and verify their remaining CIP-003 R5 related procedures and remediate identified gaps.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-003-1 R6 (RFC2012010302, RFC2013011966, NPCC2014013554)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-003-1 R6 for failing to implement supporting configuration management activities to identify, control, and document all changes to a set of CCAs pursuant to its change control process. Specifically, URE2 failed to follow all of its change control processes for a set of computers and computer consoles classified as CCAs. ReliabilityFirst confirmed that these facts and circumstances constituted a violation during the URE2 Compliance Audit.

Subsequently, URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, URE3 did not have sufficient evidence to demonstrate that it implemented supporting configuration management activities to identify, control, and document all changes to CCAs pursuant to its change control process.

ReliabilityFirst determined that URE2 and URE3 had violations of CIP-003-1 R6 for failing to implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of CCAs pursuant to their change control processes.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on URE2 and URE3 through when URE2 and URE3 completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure of URE2 and URE3 to identify, control,

and document all entity or vendor-related changes to CCA hardware or software could have increased the possibility of system outages or downtime associated with unauthorized and/or undocumented changes. However, URE2 and URE3 provided certain security management controls to protect CCAs. Specifically, while some CCAs were not subject to all steps within their change control processes, all assets were subject to some aspects of the processes. Further, all assets at all times resided within the defense-in-depth perimeters, which included layers of firewall protection and monitoring within the Electronic Security Perimeters (ESPs) and PSPs.

URE2's Mitigation Plan and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required URE2 and URE3 to:

1. reinforce the proper implementation of existing change control processes to appropriate personnel;
2. ensure that previously excluded CCAs were subjected to the change control procedures;
3. revise the change control process document; and
4. perform a quality assessment with an action plan to address lessons learned from the quality assessment with the appropriate personnel.

URE2 and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-004-1 R3 (RFC2012010303 and NPCC2014013550) and CIP-004-3a R3 (RFC2012011364 and RFC2014013316)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-004-1 R3 for failing to update the PRA for one contractor at least every seven years after the initial PRA, and for failing to revoke this contractor's access between the expiration and subsequent renewal of the contractor's PRA. Additionally, during the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to include a provision requiring URE2 to update each PRA for cause in its documented PRA program.

Subsequently, URE3 submitted a Self-Report to ReliabilityFirst stating that it failed to update the PRA for five employees at least every seven years after the initial PRA.

URE1 later submitted a Self-Report to ReliabilityFirst stating it failed to update the PRAs for six employees every seven years after the initial PRA.

URE2 later reported that it failed to update the PRAs for four employees in addition to the previously-identified contractor.

ReliabilityFirst determined that URE2 had a violation of CIP-004-1 R3 for failing to update the PRA for one contractor and four employees at least every seven years. ReliabilityFirst determined that URE3 had a violation of CIP-004-3a R3 for failing to update the PRA for five employees. ReliabilityFirst determined that URE1 violated CIP-004-3a R3 for failing to update the PRA for six employees.

ReliabilityFirst determined the duration of URE2's violation to be from the date the Standard became mandatory and enforceable on URE2 through when URE2 completed its Mitigation Plan. ReliabilityFirst determined the duration of URE3's violation to be from the date of URE3's earliest identified noncompliance through when URE3 completed its Mitigation Plan. ReliabilityFirst determined the duration of URE1's violation to be from the date of URE1's earliest identified noncompliance through when URE1 completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. For the URE2 violation, the contractor's PRA was late by 31 days, and URE2's existing access monitoring processes immediately identified and escalated the issue. The contractor was a trusted vendor who had a previously-valid PRA, and the renewed PRA indicated no PRA-disqualifying factors. Further, the contractor was a member of a well-known and widely-used vendor managed security services staff. URE2 had external audit results that demonstrated the effective design and operation of the vendor's controls. Lastly, URE2 required PRAs for all contractors and employees who needed access to CCAs, even though its documentation was lacking. URE2 has experienced no instances of "for cause" situations since the date of mandatory compliance.

In relation to the URE Companies' failures to update employee PRAs in a timely manner, once identified, the URE Companies immediately removed the access for the employees with expired PRAs and subsequently updated each PRA. The URE Companies instituted manual processes to ensure timely PRAs until they could remedy the issues they experienced with their automated system that led to these violations. Further, the URE Companies used their monitoring and detective controls and verified that these individuals did not conduct inappropriate activities during the time their PRAs were expired.

URE3's Mitigation Plan and URE1's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required URE3 and URE1 to:

1. remove access for all employees with expired PRAs;

2. develop additional guidance for personnel entering PRA data into the human resources systems;
3. reprogram their systems to prevent future transposing of PRA data;
4. correct the PRA data entry errors for the individuals with access; and
5. train personnel on the proper insertion of PRA data into their systems.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst stating it had been completed.

In addition to completing the steps also undertaken by URE3 and URE1, URE2's Mitigation Plan required URE2 to:

1. renew the PRA for the contractor;
2. update its PRA procedure to include the renewal of PRAs for cause; and
3. replace vendor-managed firewalls with URE Company-managed firewalls to ensure appropriate management of access control and PRA processes for the affected assets.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-004-1 R4 (RFC2012010080, RFC2012010087, RFC2012010094, NPCC2014013549)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-004-1 R4 for failing to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, the URE Companies failed to include all of their information technology (IT) administrators on their list of personnel with authorized access to CCAs because these individuals gained access through their addition to groups that gave them access privileges, instead of through the standard access review and approval process.

During the URE2 Compliance Audit, URE2 failed to provide evidence demonstrating that it conducted a quarterly review of the lists of its personnel with access to CCAs, nor was it able to provide evidence that it updated the lists within seven calendar days of any change.

URE3 subsequently reported that it failed to remove an individual from its list of individuals with physical access to CCAs until five days after removal was required. URE3 discovered this issue during its quarterly review of the lists of personnel with access to CCAs.

During the URE1 Compliance Audit, URE1 failed to provide evidence demonstrating that it properly maintained the list of personnel with authorized cyber or authorized unescorted physical access to CCAs. Instead, URE1 provided an access list which did not include specific electronic access rights for all personnel with cyber access. Following the URE1 Compliance Audit, URE3 reported that it also failed to maintain sufficient evidence demonstrating the specific access rights of personnel with access to CCAs.

ReliabilityFirst determined that the URE Companies had violations of CIP-004-1 for failing to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies trained and conducted PRAs on all IT administrators and granted each with access through local area network IDs and password credentials. In addition, while the access lists did not contain all of the required information, the URE Companies did maintain access lists with some of the required information. Further, the URE Companies implemented authorization criteria for all individuals accessing CCAs, including PRA and training requirements, and record basic access information. Lastly, URE3 retrieved the access badge of the individual who no longer required physical access to CCAs. Therefore, while the individual remained on the access list, the individual did not have the ability to access the area.

URE1's Mitigation Plan and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst stating it had been completed.

The Mitigation Plans required the URE Companies to:

1. define access group ownership;
2. add appropriate individuals to the asset lists;
3. perform a quality assessment review of existing practices for maintaining authorized access lists; and
4. implement enhancements to their existing processes for maintaining authorized access lists.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-005-1 R1 (RFC2012010305, RFC2012010924, RFC2013011967, NPCC2014013440)

URE2 submitted a Self-Report to ReliabilityFirst stating that it had a violation of CIP-005-1 R1 for failing to identify and document two devices that would permit access up to the ESP. Subsequently, during the URE2 Compliance Audit, ReliabilityFirst discovered additional instances of noncompliance. Specifically, URE2 failed to: (i) identify an access point to its ESP within its ESP diagram; (ii) maintain sufficient evidence to demonstrate that it afforded any of the protective measures specified in CIP-005-1 R1.5 to its firewall management device (a Cyber Asset used in the access control and monitoring of the ESPs), and (iii) reflect revision history or version maintenance on its ESP diagrams.

Subsequently, URE1 submitted a Self-Report to ReliabilityFirst stating that it could not establish that it had identified all access points to the ESPs and could not establish that it afforded the protective measures specified in CIP-005-1 R1.5 to all Cyber Assets used in the access control and monitoring of the ESPs. During the URE1 Compliance Audit, ReliabilityFirst determined that URE1 also failed to ensure and document that every CCA resides within an ESP and failed to identify and document all ESPs (R1 and R1.6). Further, ReliabilityFirst identified that, in several of the instances self-reported by URE1 involving URE1's failure to identify access points, URE1 failed to consider communication links terminating at end points within defined ESPs as access points to the ESPs (R1.3).

Later, URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it did not have sufficient evidence to demonstrate compliance with CIP-005-1 R1. Specifically, URE3 could not demonstrate that it: (i) identified access points to the ESP; (ii) identified and protected non-critical Cyber Assets within a defined ESP; (iii) afforded the protective measures specified in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESPs; or (iv) maintained documentation of all electronic access points to the ESPs.

Subsequently, URE2 reported that it did not have sufficient evidence to demonstrate that it provided all CIP-005 protections to a set of printers within an ESP, as required by CIP-005-1 R1.4.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R1 for failing to identify access points to the ESP, afford the protective measures specified in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP, maintain documentation of the ESP and all electronic access points to the ESP, and identify and protect non-critical Cyber Assets within a defined ESP.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to identify all access points to the ESPs and provide them with the required protections increased the possibility of unauthorized electronic access to CCAs and non-critical Cyber Assets, potentially resulting in system misuse or compromise.

However, the URE Companies did implement measures to provide protections to ESPs, access points to ESPs, Cyber Assets used in the access control and monitoring of the ESPs, and CCAs. The URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy.

In addition, although the affected devices may not have been subject to certain CIP-005-1 R1 required procedures, they were subject to general access processing and change control requirements, which provide security for the system by limiting unauthorized access and protect against unexpected or unauthorized changes based on existing processes.

With respect to URE1's violation, URE1 applied CIP-005-1 R1 requirements, with the exception of documenting the access points on its ESP diagram. URE1 initially classified two types of access points only as CCAs instead of CCAs and electronic access points; as CCAs, they were afforded all CIP protections. Further, these access points do not allow interactive access into the device or the ESP.

With respect to URE3's violation, URE3 misclassified access points to the ESP as either CCAs or other types of assets requiring protection, applying applicable protections to those devices.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise existing documentation and develop additional documentation and guidance for the classification of electronic access points to the ESP, non-critical Cyber Assets, Cyber Assets used the access control and monitoring of the ESPs, and protected Cyber Assets;
2. use the revised and newly-added documentation to identify appropriate assets and update all ESP diagrams;

3. perform an analysis of the identified assets for required CIP controls based on their classification and implement the appropriate CIP protections on each asset; and
4. provide appropriate communication and training on these changes to personnel.

CIP-005-1 R2 (RFC201100890, RFC201100897, RFC201100904, NPCC2014013551)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R2 for failing to ensure the authenticity of an accessing party in situations where they had enabled external interactive access into the ESP and for failing to document the technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP.

The URE Companies permitted external vendors performing IT support functions to use a single generic user identification. As a result, the URE Companies were unable to determine the identity of a specific person accessing the ESP and consequently could not ensure the authenticity of the accessing party. Additionally, the URE Companies permitted external interactive access to the ESPs through the use of a reporting tool. Once a user installed the tool, it could access the ESP. The URE Companies did not implement authentication controls on this tool. In one instance, a user accessing the application had access to an information repository hosted on a CCA, but the URE Companies had not first ensured the authenticity of this individual.

The URE Companies also did not implement their technical and procedural mechanisms for control of remote access to the supervisory control and data acquisition (SCADA) system. The URE Companies have a process for control of electronic access at electronic access points to the ESP, but this process was not implemented for remote access to the SCADA system. Specifically, the URE Companies did not document the continuous monitoring of a vendor performing SCADA IT work as specified within the URE Companies' organizational processes and technical and procedural mechanisms for control of electronic access.

Subsequently, the URE Companies reported that IT administrators were able to bypass the URE Companies' controls and gain access to CCAs within an ESP through the use of an active directory authentication control. URE2 also self-reported that it failed to identify and document two devices that would permit access up to the ESP.

During the URE2 Compliance Audit, ReliabilityFirst determined that a previous Self-Report for a violation of CIP-007-1 R2 also indicated noncompliance with CIP-005-1 R2. Specifically, URE2 did not document that it only enables ports and services required for operations and monitoring as required by CIP-005-1 R2.2. URE2 stated that it does not perform firewall rule set reviews for validity once a firewall rule is approved and implemented.

During the URE1 Compliance Audit, URE1 stated that its previously self-reported CIP-007-1 R2 violation also indicated a violation of CIP-005-1 R2. Specifically, URE1 did not document that it only enables ports and services required for operations as required by CIP-005-1 R2.2.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R2 for failing to document and implement organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the inconsistent application of organizational processes and technical and procedural mechanisms for controlling electronic access at all electronic access points to the ESP could have left access points, and therefore the ESP, exposed to unauthorized access and vulnerable to cyber intrusion.

However, the URE Companies implemented measures to provide protection to Cyber Assets within the ESP, as well as to access points to the ESP. First, the vendor personnel using the generic identification were required to authenticate to the URE Companies' environments before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred. Further, all personnel assigned to the generic user identification had completed PRAs and CIP training. Second, access to the reporting tool was limited to those individuals with authorization to access the corporate domain, the application itself, or a link to the application, and access to the tool from within the corporate network.

Third, while IT administrators were able to access CCAs within an ESP through the active directory authentication control, only the local IT administrators were able to use this access, and each of these users had network access credentials and received training and PRAs.

Fourth, while the URE Companies' documentation was insufficient, the URE Companies did secure their SCADA networks and had implemented remote access processes and controls.

Fifth, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

Lastly, in relation to the ports and services issue, the URE2 and URE1 violations related to the proper documentation of baselining of open ports and services accompanied by the operational and business need for those ports and services to be open. The URE Companies followed a formal process for review, approval, and implementation of firewall rules. The firewalls deny access by default, and dial-up access to or within the ESP is not permitted by policy. The URE Companies also perform routine vulnerability assessments for the affected devices, although their documentation was lacking appropriate details to establish compliance in certain instances.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise and add documentation and guidance for the classification of electronic access points to the ESP, non-critical Cyber Assets, Cyber Assets used in the access control and monitoring of the ESPs, and protected Cyber Assets;
2. use the revised and newly-added documentation to identify appropriate assets and update all ESP diagrams;
3. perform an analysis of the identified assets for required CIP controls based on their classification and implement the appropriate CIP protections on each asset;
4. remove the reporting tool application from the ESP;
5. implement updates to existing processes, technical mechanisms, and current procedural documentation;
6. review prior baselining of ports and services;
7. develop a new process for the baselining of ports and services;
8. conduct a baselining of ports and services for each Cyber Asset; and
9. provide appropriate communication and training on these changes to personnel.

CIP-005-1 R3 (RFC201100891, RFC201100898, RFC201100905, NPCC2014013548)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R3 for failing to implement an electronic or manual process for monitoring and logging access points to the ESPs at all times. Specifically, the URE Companies allowed external vendors to remotely access CCAs through the use of one generic identification for multiple individuals, while being monitored by an employee. More than one person was able to use the same identification; as a result,

the URE Companies could not authenticate or log the specific person accessing a CCA at a given access point.

Subsequently, the URE Companies self-reported that they failed to implement a process for monitoring and logging when IT administrators were able to access ESPs through an active directory authentication tool which did not monitor and log access. URE2 also reported that it failed to implement and document processes at two devices identified as CCAs with dial-up accessibility.

The URE Companies also reported that, in the process of implementing mitigating activities to address their noncompliance with CIP-005 R3, they discovered that they were not subjecting certain firewall devices to existing logging, monitoring, and alerting processes. Since the logs did not exist, the URE Companies could not perform manual reviews of logs.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R3 for failing to implement and document an electronic or manual process for monitoring and logging access at access points to the ESP at all times.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to implement processes for monitoring and logging access at access points to the ESPs provided the opportunity for individuals to access their ESPs while leaving no record of the intrusion. This increased the possibility that the URE Companies would be unable to prevent or track intrusions that could result in harm to the integrity of the CCAs within the ESPs.

However, the URE Companies did implement measures to detect and alert for unauthorized access to their ESPs and to protect Cyber Assets within the ESP as well as access points to the ESP.

First, the vendor personnel using the generic identification were required to authenticate to the URE Companies' environments before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred. Further, all personnel assigned to the generic user identification had completed PRAs and CIP training. Second, while IT administrators were able to access CCAs within an ESP through the active directory authentication control, only the local IT administrators were able to use this access, and each of these users had network access credentials and received training and PRAs. Third, while the URE Companies' documentation was insufficient, the

URE Companies did secure their SCADA networks and had implemented remote access processes and controls.

Fourth, URE2's ESP firewalls have a deny-by-default policy. URE2 requires that access be requested through its firewall change request process. Access, if approved, is granted through the firewalls based on source IP address, destination IP address, and destination ports as requested. Personnel verify that users requiring interactive access into the ESP have a background check and CIP training before granting access.

Lastly, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. revise active directory group ownership and add new groups to assets where necessary;
2. document the practices for electronic remote access into the ESP;
3. implement updates to existing processes, technical mechanisms, and current procedural documentation; and
4. perform quality assurance reviews of account logging and monitoring on checkpoint firewalls to confirm authentication methods and their ability to log and monitor activity appropriately.

CIP-005-1 R4 (RFC2012010297, RFC2012010311, RFC2012010314, NPCC2014013541)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they each had violations of CIP-005-1 R4 for failing to conduct a review to verify that only ports and services required for operations at the access points are enabled during their annual CVA of the electronic access points to the ESPs. Additionally, the URE Companies failed to maintain documentation demonstrating that their annual CVAs include a document identifying the vulnerability assessment process, the discovery of all access points to the ESP, a review of controls for default accounts, passwords, and network management community strings, and documentation of the results of the assessment, the action plan

to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

In addition, during the URE2 Compliance Audit, URE2 failed to provide evidence to demonstrate that a vulnerability assessment plan existed, as required by its CVA process. ReliabilityFirst also discovered that URE2's CVA process does not require URE2 to document the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, or the execution status of that action plan. Finally, URE2 failed to submit evidence to demonstrate compliance with any of the remaining sub requirements of CIP-005-1 R4.

ReliabilityFirst determined that the URE Companies each had violations of CIP-005-1 R4 for failing to maintain documentation that they performed an annual CVA of the electronic access points to the ESPs that included each of the required provisions.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to conduct compliant CVAs increased the possibility that the URE Companies would be unaware of discoverable and preventable cyber vulnerabilities, and that an individual could exploit these vulnerabilities to gain unauthorized access to CCAs within the ESPs.

However, the URE Companies did implement protections to reduce the risk of unauthorized access to the ESPs. Although the URE Companies did not document the implementation of CVA requirements as defined in CIP-005-1 R4, they were conducting vulnerability scanning through a vulnerability scanning program. In addition, the URE Companies provide all cyber assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. review prior baselining and develop a new process for the baselining of ports and services;
2. conduct a baselining of ports and services for each Cyber Asset;

3. revise their documented CVAs and annual review processes to develop CIP-specific processes and supporting documentation for CVAs; and
4. perform an annual review of in-scope documentation and an annual CVA.

CIP-005-1 R5 (RFC2012010298, RFC2012010310, RFC2012010315, NPCC2014013534)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-005-1 R5 for failing to annually review, update, and maintain all documentation to support compliance with the requirements of Reliability Standard CIP-005. The reviews of program documents were not completed in a timely manner.

During the URE2 Compliance Audit, ReliabilityFirst also discovered that the URE2 ESP diagrams did not reflect revision history or version maintenance to demonstrate that URE2 maintained the ESP diagrams as required.

ReliabilityFirst determined that the URE Companies had violations of CIP-005-1 R5 for failing to annually review, update, and maintain all documentation to support compliance with the requirements of CIP-005.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies have documented processes requiring the annual review and approval of CIP-related documentation. These violations reflected documentation deficiencies related to the URE Companies' workflow processes and the inability to produce evidence of annual task completion.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to update existing processes, technical mechanisms, and current procedural documentation, and perform an annual review of in-scope documentation.[4]

[4] In addition, as part of the overall mitigation work, the URE Companies have made significant improvements to the annual review and documentation processes.

CIP-006-3c R1 (RFC201100892, RFC201100899, RFC201100906, NPCC2014013536)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-006-3c R1 for failing to implement their visitor control programs documented in their physical security plans. Specifically, the URE Companies reviewed instances where employees and contractors without authorized unescorted access to PSPs entered the PSPs without an escort.

During the URE2 Compliance Audit, URE2 failed to provide sufficient evidence to demonstrate that the physical security plan is reviewed at least annually and approved by the senior manager or delegate. ReliabilityFirst also discovered that, while URE2 identified all physical access points through each PSP and measures to control entry at those access points, URE2 did not include this information within its physical security plan. Further, ReliabilityFirst discovered that URE2 failed to ensure that all Cyber Assets within an ESP also reside within a defined PSP, when a completely enclosed six-wall border could not be established for Ethernet network cabling for CCAs. No Technical Feasibility Exception (TFE) was submitted.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-3c R1 for failing to implement a physical security plan that addresses a visitor control program mandating escorted access of visitors within the PSP, and for failing to document, implement, and maintain a physical security plan, approved by a senior manager or delegate, that addresses the sub-requirements of the Standard.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to document, implement, and maintain a physical security plan addressing the sub-requirements of R1 increased the possibility that an individual could physically access, misuse, or compromise Cyber Assets that were not protected. Further, individuals without proper authorization and proper escort gained access to PSPs.

However, the risk was mitigated by several factors. In each instance related to the visitor access program, the issues involved existing employees or contractors, many of whom were in the process of being authorized. None of the instances involved a malicious attempt to access a restricted area. Further, the URE Companies provided protections to control a visitor's access to PSPs. These protections included door alarms and security notifications, which were working during the period of the violations. In addition, each PSP area was monitored by security personnel through cameras and alarm systems.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required the URE Companies to:

1. develop guidance for visitor access;
2. update their visitor access procedures and associated training modules;
3. develop a formal security guidance document for minimal security controls for restricted areas;
4. revise signage practices for restricted areas;
5. assess physical access control equipment at each restricted area;
6. develop a guidance document that provides standard inspection requirements to be used at all restricted areas; and
7. train relevant personnel on these changes.

In addition, URE2's Mitigation Plan required URE2 to:

1. move assets housed in the areas identified in the URE2 Compliance Audit findings; and
2. decommission those areas and update its PSP diagrams to reflect the decommissioning.

The URE Companies certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-006-2 R2.2 (RFC2014013703, RFC2014013708, RFC2014013709, NPCC2014013535)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-006-2 R2.2 for failing to afford the protective measures required in the Standard to some newly-identified physical access control system (PACS) devices, which are devices that authorize and log access to the PSPs.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-2 R2.2 for failing to afford the protective measures specified in the Standard to Cyber Assets that authorize and/or log access to the PSPs.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies until mitigated.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to provide the protections of CIP-006 R2.2 to the PACS devices increased the possibility that unknown or unauthorized individuals could physically access CCAs, resulting in the misuse or compromise of the CCAs.

However, the URE Companies did provide some protections to limit the risk posed to their PACS devices. The newly-identified PACS devices are located inside a PSP and further locked inside cabinets therein. Electronic access to those devices is limited by default to only those individuals that had access to other PACS devices that the URE Companies protected in accordance with CIP-006-2 R2.2. The URE Companies did not identify any instances of deliberate attempts to circumvent physical access controls. Further, the URE Companies provide all assets a baseline level of protections based on the URE Companies' corporate policies and procedures and defense-in-depth security strategy. The PACS devices were provided protections such as access processing and change control requirements.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans require the URE Companies to:

1. analyze the CIP controls required for the newly-identified PACS devices and implement the controls on the devices;
2. ensure personnel with access to the devices had current PRAs and training, and retrain the personnel on the change made to the PACS devices;
3. assess the need for TFEs on technically-infeasible controls;
4. design and implement the controls required for the PACS devices; and
5. perform a quality assurance assessment to verify the controls for these devices are operating as intended.

CIP-006-3c R6 (RFC201100893, RFC201100900, RFC201100907)

The URE Companies submitted Self-Reports of CIP-006-3c to ReliabilityFirst stating that they had violations of CIP-006-3c R6 for failing to implement technical and procedural mechanisms for logging physical entry at all access points to the PSPs. Specifically, the URE Companies reviewed incidents where personnel entered restricted areas, which were defined PSPs, without appropriate access rights

or an escort. Additionally, URE3 identified one instance of intermittent door lock failures to a PSP door.

ReliabilityFirst determined that the URE Companies had violations of CIP-006-3c R6 for failing to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSPs in accordance with the Standard.

ReliabilityFirst determined the duration of the violations to be from the date of each of the URE Companies' earliest identified noncompliance through when each of the URE Companies completed the mitigating activities necessary to remedy its violation.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to implement and document the technical and procedural mechanisms for logging physical entries at their PSPs increased the possibility that unauthorized individuals could gain physical access to Cyber Assets.

However, the instances where individuals gained access involved existing employees or contractors who were either in the process of being authorized and believed themselves already to have proper authorization or who would have been escorted had they understood the area to be a restricted area. None of the instances involved a malicious attempt to access a restricted area. Additionally, all door alarms and security notifications were functional at the time of the violations, and each area was monitored by security personnel through the use of cameras and alarm systems.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address their violations were submitted to ReliabilityFirst stating they had been completed.

The Mitigation Plans required the URE Companies to:

1. develop guidance for visitor access;
2. update their visitor access procedure and associated training modules;
3. develop a formal security guidance document for establishing minimal security controls for restricted areas;
4. revise signage practices for restricted areas;
5. assess physical access control equipment at each restricted area;
6. develop a guidance document that provides standard inspection requirements to be used at all restricted areas; and

7. train relevant personnel on the changes.

URE1, URE2, and URE3 each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-007-1 R1 (RFC201100894, RFC201100901, RFC201100908, NPCC2014013546)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls. While the URE Companies reported that they conducted significant testing on changes, the URE Companies could not establish that this testing ensured that changes did not adversely impact cybersecurity controls.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies make very few significant changes to CCAs on an annual basis. Further, the URE Companies completed all changes in accordance with a change control process that includes risk-based testing, and they test all changes in a quality assurance environment before they implement the change on the CCA. All Cyber Assets within the ESP resided within defense-in-depth perimeters, including layers of firewall protection and monitoring for events within the ESPs and PSPs. Additionally, some Cyber Assets are not connected to the internet.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plan required the URE Companies to:

1. revise their definition of a significant change;
2. update their test procedures;
3. develop a checklist, by asset type, for testing cybersecurity controls when a significant change occurs;

4. train relevant personnel on the revised checklist and processes;
5. perform an assessment to determine whether the revised processes and checklists were followed during a significant change; and
6. develop recommended actions based on the assessment of the implementation of the revised processes and procedures.

CIP-007-1 R2 (RFC201100895, RFC201100902, RFC201100909, and NPCC2014013545)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R2 for failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. Specifically, the URE Companies reported that they conducted testing on Cyber Assets and determined that they were unable to confirm that only ports and services required for normal and emergency operations were enabled.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R2 for failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure increased the possibility that unauthorized network traffic could infiltrate the ESP through ports and services that are not necessary for normal or emergency operations but nevertheless remain enabled.

However, the URE Companies provided some protections to their systems to reduce the risk of vulnerabilities. First, the URE Companies provided periodic vulnerability scans to identify open ports and services and then evaluated and managed any issues through the scanning process. Second, the URE Companies used vulnerability scanning to identify vulnerabilities within the ESP that, when closed through vulnerability assessment remediation, effectively keep the systems within the ESP more hardened related to patching, closing unneeded or vulnerable services, and upgrading unsupported or vulnerable systems. Third, the URE Companies reviewed all ESP and CCA ports during initial implementation. Fourth, the URE Companies encompass ESPs with additional electronic perimeters, separating the real-time networks from the corporate network and the internet. These electronic

perimeters are monitored by an intrusion detection system (IDS). Lastly, all Windows assets have antivirus software installed.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review prior baselining of ports and services;
2. develop a new process for the baselining of ports and services; and
3. conduct a baselining of ports and services for each Cyber Asset.

CIP-007-1 R3 (RFC2012010081, RFC2012010088, RFC2012010095, NPCC2014013544)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R3. Specifically, the URE Companies failed to follow the corporate patch management program for certain devices. The URE Companies also reported that they were unable to demonstrate that they assessed certain patches for applicability within 30 calendar days of availability. URE1 also reported that for one Cyber Asset, it was not technically feasible to install the patch, but URE1 failed to document the compensating measures applied to mitigate risk exposure or acceptance of the risk.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to demonstrate that it assessed patches for applicability for certain devices and applications within 30 calendar days of availability.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R3 for failing to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability. In addition, ReliabilityFirst determined that URE1 had a violation of CIP-007-1 R3 for failing to document compensating measures applied to mitigate risk exposure or an acceptance of the risk in one instance where a patch was not installed.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to follow their patch management programs increased the possibility that unauthorized network traffic could infiltrate the

ESP or that a malicious individual could exploit known vulnerabilities. However, several factors mitigated the risk during the duration of the violations.

All Cyber Assets within the URE Companies' ESPs resided within defense-in-depth perimeters, including layers of firewall protection and monitoring for events within the ESPs and PSPs. Some Cyber Assets are not connected to the internet.

URE1 was performing patch assessment and regular quarterly patching on a certain set of operating system assets throughout the compliance period. Prior to applying patches to all production assets, URE1 first applies patches to non-production assets that are not CCAs and which are segregated from the critical production assets in a quality assurance system environment. URE1 then performs functional and cybersecurity control testing and approval cycles. After this step, it then applies patches to lower-risk production assets before applying the patches to all production assets.

The URE Companies began regularly reviewing and implementing patches for most key elements, such as operating systems and crucial SCADA applications, during the compliance period.

URE2 began actively patching its remote terminal unit platforms and certain operating system units during the compliance period. Similar to URE1, URE2 first performs patching against non-production assets.

URE1 began actively monitoring, evaluating, and patching other key systems during the compliance period.

URE3 has performed assessments of released patches every 30 days beginning during the compliance period.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. update their patch management program, management model documents, and TFE filings;
2. determine which software should be subject to patch management processes;
3. design processes to monitor the release of vendor patches;
4. develop a process for alerting responsible personnel when vendor patches are released;

5. train appropriate personnel on implemented processes to ensure monitoring and patch reviews are occurring as expected; and
6. implement any remaining corrective actions based on the results of the assessments.

CIP-007-1 R4 (RFC2012010082, RFC2012010089, RFC2012010096)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R4. Specifically, the URE Companies failed to implement their processes for implementing antivirus and malware updates, including the requirements within those processes that mandate the testing and installation of signature files. In certain instances, the URE Companies encountered technical issues with the server's operating system, which was not able to support certain automatic updates. In those cases, the URE Companies did not document compensating measures applied to mitigate risk exposure or an acceptance of the risk.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 did not install antivirus and malware prevention tools on a different server. ReliabilityFirst also discovered that URE2's process documentation did not address the testing of antivirus signatures for two sets of devices which are Cyber Assets within an ESP.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R4 for failing to document and implement antivirus software and other malware prevention tools on all Cyber Assets within the ESPs and by failing to implement a process for the update of antivirus and malware prevention signatures.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to ensure that all required devices implemented antivirus software and had updated signature files in place increased the possibility that malware could be introduced, exposed, and propagated on Cyber Assets within the ESP.

However, several factors mitigated the risk. First, the URE Companies used IDS to monitor all network traffic and compare aggregate traffic against known malicious signatures. All of the URE Companies' Cyber Assets are housed deep within the network infrastructure, which is isolated from typical

malware attack vectors. Email clients were not installed on these Cyber Assets, and the Cyber Assets did not have access to the internet.

In addition, the URE Companies provide all Cyber Assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

Lastly, each instance of noncompliance with CIP-007-1 R4 was limited in scope.[5] These issues related to the URE Companies' failures to test signature files due to vendor errors in testing, apply compensating measures for technically infeasible malware application, and install antivirus and malware software on a single device inside an ESP that was not a CCA.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. perform a quality assurance review and assessment of existing antivirus and malware operations to identify compliance gaps;
2. assess their devices for necessary TFE filings;
3. implement technical solutions necessary to ensure compliance with the Standard; and
4. assess devices again to verify compliance.

CIP-007-1 R5 (RFC2012010083, RFC2012010090, RFC2012010097, NPCC2014013537)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R5. Specifically, the URE Companies failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

The URE Companies granted certain IT administrators access to Cyber Assets through authentication groups, which gave them access outside of the required approval process. The URE Companies also failed to require password changes for certain firewalls, routers, and switches on the 90-day interval required by their own processes. The URE Companies also failed to review user accounts to verify that access privileges are in accordance with CIP-003 R5 and CIP-004 R4 on an annual basis; several of these

[5] ReliabilityFirst considered the aggregate effect of each of these violations to pose a moderate risk to the reliability of the BPS, but considered each individual instance to be limited in scope.

reviews were completed late. The URE Companies reported that they were also in violation of CIP-007-1 R5.2, when they assigned generic administrator accounts to IT support personnel, but failed to authenticate specific individuals on login. The URE Companies also failed to authorize formally access to shared accounts in certain instances. Lastly, the URE Companies reported that they failed to enforce password complexity and frequency changes for certain Cyber Assets.

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 also failed to generate logs to create historic audit trails of individual user access activity for a minimum of 90 days for sampled devices and Windows platforms. URE2 failed to demonstrate that it implemented an annual review of user accounts to verify access privileges in accordance with CIP-007-1 R5.1.3. Lastly, ReliabilityFirst discovered that URE2 failed to have a policy for managing the use of shared accounts that includes a provision requiring an audit trail of the account use and steps for securing the account in the event of personnel changes, as required by CIP-007-1 R5.2.3.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R5 for failing to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to implement technical and procedural controls increased the possibility of unauthorized system access, potentially resulting in system misuse or compromise.

However, several factors mitigated the risk. First, each of the IT administrators had received training and PRAs and had approved network access credentials. Second, the URE Companies required the IT support personnel using the generic user identification to first authenticate to the corporate environment. All personnel had PRAs and CIP training, and the URE Companies monitored their work as it occurred.

Third, the URE Companies were performing some annual reviews and properly managing user account privileges, although these reviews did not meet all the requirements of CIP-007-1 R5. The URE Companies revoke physical and electronic access upon termination of an employee, and changing roles triggers an action to review continued business need and access required. The URE Companies also

implemented automated processes to initiate notifications when an individual's PRA or training is about to expire.

Fourth, the URE Companies provide all assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by the failure to implement password changes and the failure to implement logging and monitoring on some network switches.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plan required the URE Companies to:

1. change all passwords for any device identified as not having met the frequency or complexity requirements;
2. implement interim manual processes to ensure password change frequency and complexity requirements are met;
3. review current ESP electronic access point access request, authorization, and authentication practices against existing formal procedures;
4. revise active directory groups ownership and add new groups to assets where necessary;
5. update existing processes, technical mechanisms, and current procedural documentation;
6. implement tools and technologies for user-level authentication;
7. revise TFEs as necessary;
8. complete a monitoring assessment of generic ID usage procedures;
9. perform a quality assurance review of account logging and monitoring on checkpoint firewalls and network switches;
10. implement a solution to enforce monitoring and logging;
11. identify opportunities and lessons learned to enhance the existing process for reviewing access to user accounts;
12. train relevant personnel; and
13. perform a peer quality assessment of annual user privileges in accordance with designated processes and develop a plan for implementing lessons learned.

CIP-007-1 R6 (RFC2012010084, RFC2012010091, RFC2012010098, NPCC2014013543)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R6. The URE Companies reported that they failed to log properly system events related to cybersecurity for CCAs, other types of protected assets, and access control and monitoring assets.

During the URE2 Compliance Audit, URE2 failed to provide evidence that it performs monitoring of security events as required by its organizational processes and technical and procedural mechanisms. URE2 also failed to provide evidence establishing that it issues alerts for detected Cyber Security Incidents.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R6 for failing to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to log system events related to cybersecurity increased the possibility that undetected misuse or compromise of CCAs and other system events that are related to cybersecurity could occur without the URE Companies' knowledge.

However, several factors mitigated the risk. First, although IT vendor personnel were permitted to use a generic user identification, the personnel were required to first authenticate to the corporate environment before accessing electronic access points to the ESP. The URE Companies monitored the vendors' work as it occurred, and all personnel assigned to the generic identification had completed PRAs and CIP training. In addition, the lack of automated monitoring was mitigated by the URE Companies' use of manual logging and reviewing.

Additionally, the URE Companies provide all Cyber Assets with certain protective measures, based on the URE Companies' corporate policies and procedures and defense-in-depth strategy, which reduced the risk posed by these violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. update existing processes, technical mechanisms, and current procedural documentation;
2. document acceptable compensating measures for generic identifications and logging reviews;
3. implement acceptable tools and technologies for user-level authentication;
4. implement process improvements to prevent future gaps with respect to logging;
5. perform a quality assurance review of account logging and monitoring on checkpoint firewalls and network switches; and
6. implement solution to enforce monitoring and logging.

CIP-007-1 R7 (RFC2012010921, RFC2012010925, RFC2013011968, NPCC2014013542)

During the URE2 Compliance Audit, URE2 failed to present evidence demonstrating that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP.

Subsequently, URE1 submitted a Self-Report to ReliabilityFirst stating that it did not have sufficient evidence to demonstrate that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP. During the URE1 Compliance Audit, ReliabilityFirst confirmed that these facts and circumstances constituted a violation of CIP-007-1 R7.

URE3 later submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it did not have sufficient evidence to demonstrate that it established formal methods, processes, and procedures for the disposal or redeployment of Cyber Assets with the ESP.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R7 for failing to establish formal methods, processes, and procedures for disposal and redeployment of Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the violation increased the possibility that non-trained, unauthorized individuals could retrieve sensitive data from the devices.

However, the URE Companies had some protections in place to limit the potential for unauthorized retrieval of data from their Cyber Assets. First, the URE Companies stored any equipment that they removed from service in existing PSPs to limit the risk that sensitive information would be accessible to unauthorized individuals. Second, while their documentation was lacking, the URE Companies sanitized, erased, and destroyed hard drives in all equipment redeployed or removed from service.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop a unified policy and procedure to govern the disposal and redeployment of all Cyber Assets;
2. conduct a pilot of the disposal and redeployment procedure;
3. assess the procedure for additional improvements;
4. implement lessons learned into the disposal and redeployment procedure; and
5. develop and deliver training on the procedure.

CIP-007-1 R8 (RFC2012010085, RFC2012010092, RFC2012010099, NPCC2014013540)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R8. The URE Companies reported that they had incomplete lists of ports and services, which did not allow the URE Companies to verify that only ports and services required for operations of the Cyber Assets within the ESPs are enabled. Additionally, during the performance of the CVAs, the URE Companies did not retain documentation to establish compliance with the remaining sub-requirements of CIP-007-1 R8.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R8 for failing to perform an annual CVA of all Cyber Assets within the ESP that included all of the sub-requirements of CIP-007-1 R8.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failure to perform an

adequate CVA of all Cyber Assets within the ESP at least annually increased the possibility that the URE Companies' systems would be open to cyber vulnerabilities.

However, the URE Companies provided some protections to their systems to reduce the risk of vulnerabilities. Although the URE Companies did not document the implementation of CVA requirements as defined in the Standard, they were conducting vulnerability scanning through a software program. Further, the URE Companies implemented periodic vulnerability scans to identify open ports and services and then evaluated and managed any unusual issues through the scanning process.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review prior baselining;
2. develop a new process for the baselining of port and services;
3. conduct a baselining of ports and services for each Cyber Asset;
4. revise their documented CVA processes; and
5. implement the annual CVA using the revised processes.

CIP-007-1 R9 (RFC2012010313, RFC2012010301, NPCC2014013539, RFC2012010317)

The URE Companies submitted Self-Reports to ReliabilityFirst stating that they had violations of CIP-007-1 R9 for failing to review, update, and maintain all documentation to support compliance with the requirements of CIP-007 at least annually. During the URE2 Compliance Audit, ReliabilityFirst confirmed that URE2 did not maintain documentation to demonstrate a review and update of the documentation specified in CIP-007 and confirmed that these facts and circumstances constituted a violation of the Standard.

ReliabilityFirst determined that the URE Companies had violations of CIP-007-1 R9 for failing to annually review and update the documentation specified in CIP-007.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed the mitigating activities necessary to remedy the violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations were documentation deficiencies. The URE Companies had documented processes requiring the annual review and approval of CIP-related documentation. The URE Companies were not maintaining sufficient documentation of their annual reviews because their workflow processes did not provide sufficient evidence of compliance (i.e., the dates on which information was approved).

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. review and revise existing annual review processes;
2. develop systematic mechanisms to ensure that an annual review is scheduled for each year;
3. develop an inventory of all CIP-007 documentation subject to review under the revised processes;
4. plan, schedule, and perform an annual review of in-scope documentation; and
5. perform a quality assessment to ensure that all necessary documentation was included in their review processes.

CIP-008-1 R1 (RFC2012010907, RFC2012010926, RFC2013011970, NPCC2014013538)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to develop and maintain within its Cyber Security Incident response plan a process for ensuring that the plan is reviewed at least annually. Specifically, URE2 developed a stand-alone process for ensuring that the plan is reviewed at least annually, but failed to include this process within the plan itself. URE2 also failed to provide sufficient evidence to demonstrate that it performed annual reviews of the plan.

URE1 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, it was also in violation of CIP-008-1 R1 for failing to maintain sufficient evidence to demonstrate that it had completed an annual review of its plan in two prior years. During the URE1 Compliance Audit, ReliabilityFirst also determined that URE1 could not demonstrate that it performed an annual review of the plan for a third year.

URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the URE2 Compliance Audit and URE1 Compliance Audit, it was also in violation of CIP-008-1 R1. Specifically, URE3 could not establish that it conducted an annual review of its plan in two prior years.

ReliabilityFirst determined that the URE Companies had violations of CIP-008-1 R1 for failing to ensure that their Cyber Security Incident response plans are reviewed at least annually. ReliabilityFirst also determined that URE2 failed to develop and maintain within its Cyber Security Incident response plan a process for ensuring that the plan is reviewed at least annually.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through when the URE Companies completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE Companies maintained a stand-alone process for annual review. URE2's failure to incorporate the stand-alone process for annual review within its Cyber Security Incident response plan was a documentation deficiency. Although their documentation was insufficient, the URE Companies reviewed their Cyber Security Incident response plans annually and in accordance with the standalone process. In addition, no Cyber Security Incidents occurred during the period of the violations.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop standardized processes and mechanisms for annually reviewing their Cyber Security Incident response plans;
2. incorporate the standardized processes and mechanisms for annual review into the Cyber Security Incident response plans;
3. conduct an annual review and quality assessment of CIP-008 documentation in accordance with the revised processes; and
4. implement a separate formal review of all CIP documentation to provide additional protection against missed reviews.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

CIP-009-1 R1 (RFC2012010908, RFC2012010927, RFC2013011971, NPCC2014013547)

During the URE2 Compliance Audit, ReliabilityFirst discovered that URE2 failed to create and annually review recovery plans for all CCAs. Specifically, although URE2 provided parts of a recovery plan for various types of CCAs, URE2 did not supply a recovery plan that satisfied all of the requirements of a recovery plan as specified by CIP-009-1 R1. ReliabilityFirst also discovered that URE2 failed to specify, within its recovery plan a certain system, the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan, as required by CIP-009-1 R1.1.

URE1 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit, it also had a violation of CIP-009-1 R1. URE1 reported that it did not have sufficient evidence to demonstrate that it created and annually reviewed recovery plans for all CCAs. During the URE1 Compliance Audit, ReliabilityFirst confirmed that these facts and circumstances constituted a violation of CIP-009-1 R1.

URE3 submitted a Self-Report to ReliabilityFirst stating that, based on the results of the URE2 Compliance Audit and the URE1 Compliance Audit, it also had a violation of CIP-009-1 R1. URE3 reported that it did not have sufficient evidence to demonstrate that it created and annually reviewed recovery plans for all CCAs.

ReliabilityFirst determined that the URE Companies had violations of CIP-009-1 R1 for failing to create and annually review recovery plans for all CCAs. In addition, URE2 failed to specify within its recovery plan for a certain system the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable on the URE Companies through completion of the Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the URE Companies' failures to create complete recovery plans and review them on an annual basis increased the possibility that the recovery of a failed or compromised CCA could be delayed.

However, the URE Companies did implement mechanisms to protect CCAs against system events. Although the URE Companies did not create recovery plans for all Cyber Asset types, they did implement processes to provide for backup operational capabilities to an alternative site if an entire location was lost and performed periodic failover tests to ensure that operations could in fact be

switched to the alternative site. Additionally, the URE Companies implemented mechanisms to repair or replace individual asset types and to protect CCAs against system events.

URE1's Mitigation Plan, URE2's Mitigation Plan, and URE3's Mitigation Plan to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required the URE Companies to:

1. develop consolidated governing documents implementing the CIP-009 recovery plan requirements at the asset type level;
2. develop templates for documenting individual asset type recovery plans;
3. develop updated recovery plans for CIP-009 in-scope assets at the asset type level in accordance with the revised governing documentation and guidance template; and
4. develop and implement training for individuals responsible for activation and implementation of the revised recovery plans.

The URE Companies each certified that the above Mitigation Plan requirements were completed. ReliabilityFirst will verify that the Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of six hundred and twenty-five thousand dollars ($625,000) for the referenced violations. In addition, ReliabilityFirst will randomly select and perform a Spot Check on one of the three URE Companies in the future.[6] In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered one aspect of the URE Companies' compliance history as an aggravating factor in the penalty determination;
2. The URE Companies agreed to undertake a number of above-and-beyond mitigating activities (described more fully below), which ReliabilityFirst considered a mitigating factor in the penalty determination;
3. The URE Companies had an internal compliance program at the time of the violations, aspects of which ReliabilityFirst considered a mitigating factor; however, after determining the full

[6] This Spot Check will be performed with 60 days advance notice and will include: (i) an evaluation of the evidence related to the URE Companies' completion of the above-and-beyond activities described in this Notice of Penalty and the Settlement Agreement; and (ii) a review of the current state of compliance for a random sample of CIP Reliability Standard requirements.

scope of the violations and the mitigation activities, ReliabilityFirst observed that the state of the URE Companies' mitigation activities and compliance had not progressed as quickly as expected considering the number of years they had been working to resolve these violations;

4. The URE Companies self-reported a number of violations, for which ReliabilityFirst awarded partial mitigating credit;
5. The URE Companies were cooperative throughout the compliance enforcement process, for which ReliabilityFirst awarded partial mitigating credit;[7]
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations individually posed a minimal or moderate risk, and collectively posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

As noted above, the URE Companies have agreed to undertake a series of above-and-beyond mitigating activities which address the management practices that ReliabilityFirst found to be deficient and the root cause of the violations. These above-and-beyond mitigating activities are:

1. implement an annual URE Company-wide forum to address CIP compliance management model documents, present and emerging risks, and mitigating violations;
2. formation of a single office to oversee and monitor all CIP activities across the URE Companies, at a budgeted annual cost;
3. creation of dedicated positions to increase the URE Companies' ability to identify and respond to emerging risks, plan for future activities, and improve decision results, at an annual budgeted cost; and
4. implementation of technological improvements related to CIP compliance and cybersecurity, including for logging, monitoring, and alerting of CIP assets, for configuration management

[7] ReliabilityFirst considered the URE Companies' cooperation with ReliabilityFirst, as well as the collaborative and open nature of their subject matter experts, to be a mitigating factor in the penalty determination. However, ReliabilityFirst reduced this mitigating credit in light of the extended period of time it took for the URE Companies to mitigate and resolve these violations. In particular, ReliabilityFirst considered that the URE Companies routinely requested extensions of mitigation deadlines, often on or near the various due dates for mitigation milestone deliverables.

purposes, and to isolate sensitive segments from the internet and other weaknesses, at a budgeted cost above-and-beyond the costs required for baseline compliance activities.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of six-hundred and twenty-five thousand dollars ($625,000) and the non-monetary penalty of conducting a Spot Check is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 12, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by ReliabilityFirst, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of six hundred and twenty-five thousand dollars ($625,000) and the non-monetary penalty of conducting a Spot Check is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[8] *See* 18 C.F.R. § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, Ohio 44131 (216) 503-0682 (216) 503-9207 – facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Associate General Counsel and Senior Director of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, Ohio 44131 (216) 503-0689 (216) 503-9207 – facsimile niki.schaefer@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Theresa White* Associate Counsel ReliabilityFirst Corporation 3 Summit Park Dr. Cleveland, OH 44131 (216) 503-0667 (216) 503-9207 – facsimile theresa.white@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, Ohio 44131 (216) 503-0683 (216) 503-9207 – facsimile jason.blake@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Compliance and Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: The URE Companies
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID#NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of forty-five thousand dollars ($45,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

conditions of the Settlement Agreement. The violations in this Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SPP2013011798	CIP-005-1	R1	Medium/Severe	$45,000
SPP2013011799	CIP-005-1	R2	Medium/Severe	
SPP2013011800	CIP-005-1	R3	Medium/Severe	
SPP2013011801	CIP-005-1	R4	Medium/Severe	
SPP2013011802	CIP-006-1	R1	Medium/Severe	
SPP2013011804	CIP-007-1	R1	Medium/Severe	
SPP2013011805	CIP-007-1	R2	Medium/Severe	
SPP2013011806	CIP-007-1	R3	Lower/Severe	
SPP2013011807	CIP-007-1	R5	Lower/Severe	
SPP2013011808	CIP-009-1	R1	Medium/Severe	
SPP2013011809	CIP-007-3	R8	Medium/Severe	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SPP2013012355	CIP-006-1	R1	Medium/Severe	$45,000
SPP2013012356	CIP-004-3	R4	Lower/High	
SPP2013012533	CIP-006-2a	R6	Lower/Severe	
SPP2013012752	CIP-006-2	R3	Medium/Severe	
SPP2013012841	CIP-003-1	R6	Lower/Severe	
SPP2013012842	CIP-004-1	R4	Lower/Moderate	
SPP2013012844	CIP-005-3a	R5	Lower/Lower	
SPP2013012845	CIP-006-2	R1	Medium/Severe	
SPP2013013117	CIP-006-3c	R5	Medium/Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-005-1 R1 (R1.5) (SPP2013011798)

URE submitted a Self-Report stating that it did not correctly identify four devices as electronic access points to its electronic security perimeters (ESPs). Later, URE supplemented its Self-Report, explaining that it also failed to identify two receiver devices as access points to the ESP. During its review, SPP RE further determined that URE had not subjected the identified access points to the controls identified in CIP-005-1 R1.5 where technically feasible. Additionally, the access points were not afforded some of the required controls due to technical infeasibility, but they did not have a technical feasibility exception (TFE). In its original Self-Report, URE also indicated it did not afford a number of the protective measures required by CIP-005-1 R1.5 to its two servers residing outside the ESP.

SPP RE determined that URE had a violation of CIP-005-1 R1.5 for failing to identify certain devices as electronic access points to the ESPs, and for failing to afford a number of required controls and protective measures to these devices.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, with respect to the two servers, a failure to adequately secure the servers makes access credentials vulnerable to potential theft by malicious actors. Stolen access credentials could be used to gain access to the ESP, and thereby compromise network assets used to support the reliable operation of the BPS. Nevertheless, URE had instituted a number of controls to guard against unauthorized access to the servers, including housing the servers within a physical access controlled corporate data center, and limiting electronic access to the servers to information technology (IT) system administrators.

Regarding the four devices, the failure to apply appropriate controls increased the risk that a malicious actor might successfully access URE's ESP. SPP RE determined that the role and position of the devices in the URE network limited the risk posed by the inability of the devices to implement the identified technical controls. Further, each of the devices resides within a physical security perimeter (PSP).

URE's Mitigation Plan to address this violation was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. remove the servers from their role in ESP; and
2. document the devices and file TFEs.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (R2.1; R2.2; R2.4; and R2.5) (SPP2013011799)

URE submitted a Self-Report stating that it failed to request TFEs for two switches and two additional devices. Additionally, URE's energy management system (EMS) vendor was not required to authenticate itself as an accessing party at the URE ESP firewalls. Later, URE supplemented its Self-Report, stating that it also failed to request a TFE for two devices that were not capable of authenticating the accessing party, and did not subject these devices to the documentation requirements of R2.5.

During a Compliance Audit (Compliance Audit), SPP RE discovered that URE placed a jump box4 into service to facilitate interactive access into the ESP, but failed to ensure the authenticity of the accessing parties when the jump box was accessed through a utility server.

SPP RE determined that URE had a violation of CIP-005-1 R2.1, R2.2, R2.4, and R2.5 for failing to: i) request TFEs for several devices; ii) require a vendor to authenticate itself; and iii) authenticate the accessing parties to the jump box.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The vendor was required to authenticate at the URE corporate firewall before crossing the ESP firewall, and the final grant of vendor access required affirmative action by URE to allow access at the corporate firewall. URE never granted the vendor access via its corporate firewall.

The role and position of the devices at issue in the URE network limited the risk posed by the inability of the devices to implement the identified technical controls. Additionally, some of the devices at issue resided within a PSP.

Although any of the eight unauthorized employees with access to the utility server could have attempted to access the jump box, access would have been denied for lack of credentials, i.e., an approved username and password combination. Furthermore, URE continuously monitored its network with a network monitoring utility that is set to alert for unauthorized changes in network device configurations.

URE's Mitigation Plan to address this violation was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. document the devices at issue as access points;
2. request TFEs as needed;
3. establish and implement a foot patrol inspection procedure;
4. confirm that remote desktop protocol for interactive access to the ESP access point follows an encrypted connection; and

[4] A jump box is a secured computer that administrators log onto in order to gain access to other computers and administer them. The jump box is designed to provide an extra layer of security.

5. remove the utility server with multiple user accounts from being able to access the jump host.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R3 (R3.1 and R3.2) (SPP2013011800)
URE submitted a Self-Report stating that four of its electronic access points were not capable of monitoring, logging, or alerting for electronic access attempts into URE's ESP. Although access attempts to the switches were logged and monitored during electronic sessions via URE's security monitoring, analysis, and response system, no logging was occurring when IT personnel physically connected at the switches for administrative purposes. Later, URE supplemented its Self-Report, explaining that it also did not identify two devices that were not capable of monitoring, logging, or alerting for electronic access attempts at those devices.

SPP RE determined that URE had a violation of CIP-005-1 R3.1 and R3.2 for failing to monitor electronic access to four electronic access points and two devices.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The switches reside within URE's PSP and physical access to the switches would require access to the PSP. Furthermore, the EMS was receiving information related to logging and alerts. Finally, URE continuously monitors and alerts for malicious activity on its network.

URE's Mitigation Plan was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. remove switches as access points;
2. document the devices at issue as access points;
3. request a TFE as needed; and
4. establish and implement a foot patrol inspection procedure.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (R4.2, R4.3, R4.4, and R4.5) (SPP2013011801)

URE submitted a Self-Report stating that it did not implement a cyber-vulnerability assessment (CVA) process that included: i) a review to verify that only ports and services required for operations at access points were enabled; ii) the discovery of all access points to the ESP; iii) a review of controls for default accounts, passwords, and network management community strings; and iv) documentation of the results of the assessment.

URE's CVA procedure only partially satisfied the requirements of R4.3. Additionally, URE did conduct ports and services verifications during the annual review of its access point configurations.

SPP RE determined that URE had a violation of CIP-005-1 R4.2 to R4.5 for failing to perform a CVA as required by this Standard.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of a documented action plan for assessing CVA-identified vulnerabilities increased the risk that URE might fail to address vulnerabilities impacting its EMS. Additionally, failure to evaluate all access points increased the risk of potential malicious access to the URE ESP. However, URE was running scans from inside its ESP to identify all connected devices within the network, scanning active ports and services on devices, and scanning devices for vulnerabilities on an ongoing basis. During the pendency of the violation, URE was verifying the operational necessity of its enabled ports and services during its annual review of its access point configurations. Finally, URE conducted monitoring of network device hardware status, configuration, and behavior at all times.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to conduct a CVA and ensure that:

1. all ports and services were identified;
2. all access points were identified;
3. a review of controls for default accounts, passwords, and network management community strings was conducted; and
4. the assessments results were adequately documented.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (SPP2013011802)
URE submitted a Self-Report stating that its system controllers are incapable of providing a number of the protective measures controls included in CIP-007, and TFEs were not requested. Specifically, URE did not: i) enable only the ports and services required for normal operations; ii) implement security patch management; iii) implement malicious software prevention; iv) implement the required password complexity; or v) implement security status monitoring.

SPP RE determined that URE had a violation of CIP-006-1 R1.8 for failing to provide the protective controls listed above.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when SPP RE accepted URE's TFEs.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE afforded the controllers all of the protective measures specified in R1.8 that were technically feasible. Although it could not apply the measures to the controls identified in the violation, it did apply those controls to the server that manages the controllers.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to request a TFE for the controllers at issue.

CIP-007-1 R1 (R1.1, R1.2, and R1.3) (SPP2013011804)
URE submitted a Self-Report stating that: i) it did not have test procedures for third-party software; ii) it did not ensure that third-party patches which were applied did not adversely affect existing cybersecurity controls; and iii) it did not document test results for testing conducted on some of its Cyber Assets as required by R1.3.

During the Compliance Audit, SPP RE determined that URE's cybersecurity testing procedures did not require testing of software upgrades for a third-party proprietary network monitoring device located within the ESP.

SPP RE determined that URE had a violation of CIP-007-1 R1.1 to R1.3 for failing to: i) have test procedures for some devices; ii) ensure all patches would not adversely affect the controls, and iii) document the test result for some of its Cyber Assets.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement a testing process for third-party patches presented a risk that patches might be installed in the production environment prior to vetting and could adversely affect the existing cybersecurity controls. Additionally, a failure to maintain patch records decreased URE's ability to conduct after- the-fact event analysis should a patch have an adverse effect on URE's network and ensure that testing was being conducted in accordance with procedural requirements. However, URE deployed all patches in its stand-by environment initially, scanned the host and network devices in that environment, and only after identifying that no adverse effects existed did URE deploy the patches to the operational environment. This process was consistent with URE's patch management procedure.

URE's failure to test software upgrades to the network monitoring device created a risk that the implementation of the upgrades could adversely affect the security controls configured on the device, thereby making it susceptible to malicious attack. However, URE runs a vulnerability scanning utility on a daily basis to monitor for configuration changes to devices in its environment. Additionally, the network monitoring device limited the impact of this violation.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. identify all EMS hardware that is regulated by the CIP standards;
2. develop a list of all applications residing on that hardware;
3. develop a list of databases residing on that hardware;
4. identify a reliable source for security patch update information for the assets identified;
5. develop a security patch tracking mechanism;
6. develop a process to assess identified patches;
7. develop a timeline to test and implement identified patches;

8. develop a process to address applicable patches that cannot be installed due to operational impact;
9. develop a process to ensure that all patch implementations are appropriately documented; and
10. modify its change control and configuration management process to ensure the appropriate testing of proprietary systems.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R2 (R2.1 and R2.2) (SPP2013011805)
URE submitted a Self-Report stating that, although URE was aware of enabled ports and services, it had not maintained a documented baseline of those ports and services that were required for normal or emergency operations.

SPP RE determined that URE had a violation of CIP-007-1 R2.1 and R2.2 for failing to determine that only required ports and services were enabled.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, a failure to document those ports and services required for normal and emergency operations created a risk that URE would fail to disable unneeded ports and services on hosts residing within its ESP. The failure to disable such ports or services increased the attack surface available to a potential malicious actor and weakened URE's ability to identify unauthorized changes that may have occurred in the environment. Nevertheless, URE had maintained an operational awareness of the port and service changes. Additionally, the devices at issue resided behind hardened firewalls, and were guarded by updated anti-malware software.

URE's Mitigation Plan was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. create a baseline for those ports and services that were required for normal or emergency operations; and

2. review the ports and services on that baseline to ensure only the ports and services required for normal and emergency operations were enabled.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R3 (R3.1 and R3.2) (SPP2013011806)

URE submitted a Self-Report stating that it did not document a security patch management program for tracking, evaluating, testing, and installing third-party cybersecurity software patches for Cyber Assets within the ESP. Moreover, URE's patch management program did not address the assessment and installation of third-party patches. Furthermore, four patches were not assessed within 30 days of release.

SPP RE determined that URE had a violation of CIP-007-1 R3.1 and R3.2 for failing to document a patch management program for certain patches and failing to assess four patches in a timely fashion.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of a documented and formalized process for patch management creates a risk that an ad hoc approach may be relied on for patch management. Such an approach might result in missed patches or patch implementations that have not been fully vetted and that pose a risk to existing cybersecurity controls inside URE's ESP. Nevertheless, URE did demonstrate an operational awareness of its third-party patch management process. SPP RE's review determined that while the patches were operationally important, they were not patches deployed to mitigate vulnerabilities on the host operating systems.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop and implement a procedure for the tracking and evaluation of third-party security patches; and
2. assess the missed patches.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R5 (R5.1.2; R5.1.3; R5.2.3 and R5.3.2) (SPP2013011807)
URE submitted a Self-Report stating that URE did not: i) implement an audit trail for shared account use; ii) log successful individual local and domain user access attempts; and iii) enforce the required password complexity for certain accounts.

Additionally, during the Compliance Audit, SPP RE discovered an additional violation of CIP-007-1. Specifically, URE did not provide evidence that: i) the use of one shared account discovered during a CVA was reviewed or that specific users of the account were identified; ii) it reviewed access privileges for local accounts on the physical security server; iii) it maintained an audit trail of account use for the shared account discovered during the CVA; and iv) it subjected one router's user level password to the password complexity requirements.

SPP RE determined that URE had a violation of CIP-007-1 R5.1.2; R5.1.3; R5.2.3; and R5.3.2 for failing to maintain and provide evidence of its actions taken pursuant to these subrequirements.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement all the required CIP account controls diminished URE's ability to maintain an awareness of and accountability for the use of accounts and associated privileges, which could hinder URE's ability to respond to the misuse of accounts in its environment. Additionally, the failure to establish passwords meeting the complexity requirements creates a risk that the accounts could be more susceptible to brute force password attacks. However, URE grants access on a need-to-know basis, which bolsters its ability to maintain an operational awareness of changes occurring in its environment. The CVA-identified account was not normally used by URE, and its use would have been limited to three individuals.

Regarding the physical security server, the accounts URE failed to review were limited to five individuals.

Regarding URE's inability to technically enforce the required password complexity for certain accounts, URE did procedurally require the use of a password generator to establish passwords meeting the complexity requirements.

Regarding local and domain user logging, URE was logging unsuccessful account attempts and was also logging inter-system login attempts, both successful and unsuccessful.

All account access was limited to individuals who had undergone personnel risk assessments (PRA) and CIP training. Additionally, URE utilized a network scanning utility and a vulnerability scanning utility on a daily basis to detect unauthorized configuration changes on ESP network and host machines.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. implement paper-based manual logging where shared administration accounts are being used;
2. request a TFE for the inability of some applications to enforce the password complexity requirements;
3. remove the CVA-identified shared account;
4. establish detailed records of physical security server account reviews;
5. begin maintaining logs of successful local and domain account logins; and
6. change the password on the router at issue to meet the password complexity requirements.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (R1.1 and R1.2) (SPP2013011808)
URE submitted a Self-Report stating that it had not created a recovery plan for several of its physical system components.

During the Compliance Audit, SPP RE discovered an additional violation of CIP-009-1 R1.1 and R1.2. Specifically, an URE electronic access control and monitoring (EACM) device failed when its hardware was replaced. Although the EACM device was restored to its original state, URE's recovery plan did not specify the required actions to respond to events or conditions of varying duration and severity or the defined roles and responsibilities of responders for the EACM device.

SPP RE determined that URE had a violation of CIP-009-1 R1.1 and R1.2 for failing to have a recovery plan for some of its components, and for failing to specify in its recovery plan the actions necessary to recover from a failure of its EACM device.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE physical system components were designed to default to secure mode. Also, the EACM device was restored after the system failure, and URE implemented manual log review in the interim.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. create a recovery plan for the physical system components ; and
2. create a recovery plan for the EACM device.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-3 R8 (R8.2; R8.3 and R8.4) (SPP2013011809)
URE submitted a Self-Report stating that URE did not conduct a review of controls for default accounts and did not document an action plan as part of its annual CVA.

Additionally, during the Compliance Audit, SPP RE discovered an additional violation for CVAs occurring prior to the self-reported instance of noncompliance. URE's CVAs for three consecutive years each shared several deficiencies.

SPP RE determined that URE had a violation of CIP-007-3 R8.2; R8.3; and R8.4 for failing to conduct CVAs that met these subrequirements.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The lack of a documented action plan for assessing CVA-identified vulnerabilities increases the risk that URE might fail to address vulnerabilities impacting the EMS that could be maliciously exploited to the detriment of BPS operations. However, URE ran both a network scanner and vulnerability scanner that provided URE with an ongoing operational awareness of the ports and services and accounts enabled in its environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. to perform a CVA; and

2. verify that the CVA performed includes all required elements.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R1 (R1.1 and R1.3) (SPP2013012355)
URE submitted a Self-Report stating that it had designated two centers as one ESP. However, the centers did not share one PSP and were connected by a fiber optic circuit. Because a completely enclosed border could not be provided for the fiber circuit, URE was required to implement an alternative physical control measure, but did not do so.

Additionally, URE has a set of double-doors that had not been considered as an access point to a PSP, and therefore had not been subjected to the processes, tools, and procedures for monitoring physical access to the PSP.

SPP RE determined that URE had a violation of CIP-006-1 R1.1 and R1.3 for failing to provide an alternative physical control measure for the fiber circuit at issue, and failing to consider a door as being an access point to its PSP.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The fiber circuit is owned by and within the sole control of URE. The double-doors at issue were only utilized for the moving of large equipment. Additionally, the facility was manned at all times, and the doors were subject to video monitoring, thereby heightening URE's awareness of any intrusion in the environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. alarm the double doors and institute monitoring by personnel; and

2. implement a procedure, which outlined a response plan for loss of fiber continuity.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-004-3 R4 (R4.2) (SPP2013012356)
URE submitted a Self-Report stating that it failed to revoke an employee's physical access to CCAs within seven days of that employee no longer requiring access.

SPP RE determined that URE had a violation of CIP-004-3 R4.2 for failing to revoke one employee's physical access to CCAs in a timely fashion.

SPP RE determined the duration of the violation to be from the date the employee's physical access should have been revoked, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The employee was an URE employee, remained employed by URE through the violation period, and had undergone appropriate training regarding the treatment of CCAs. Lastly, the employee could only have entered the relevant PSP using his employee badge, which would have recorded his entry into the environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to revoke the employee's physical access to the CIP areas.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2a R6 (SPP2013012533)
URE submitted a Self-Report to SPP RE stating that it had placed an emergency access badge in a lower security environment to enable access from outside the PSP in the event of a medical emergency. In the event the badge were used, the associated log did not provide sufficient information to uniquely identify individuals and the time of access.

SPP RE determined that URE had a violation of CIP-006-3c R6 for failing to ensure that the log for the security badge at issue identified all individuals and the time of their access.

SPP RE determined the duration of the violation to be from the date the emergency badge at issue was activated, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The badge was located inside a facility that required corporate badge access to enter. Furthermore, use of the badge would create a log entry in URE's physical log files, thereby providing an audit trail of badge use.

URE's Mitigation Plan was submitted to SPP RE stating that it had been completed.

URE's Mitigation Plan required URE to deactivate the emergency badge.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2 R3 (SPP2013012752)

URE submitted a Self-Report to SPP RE stating it did not place two Cyber Assets used in the access control and/or monitoring of its ESP within an identified PSP.

SPP RE determined that URE had a violation of CIP-006-2 R3 for failing to place two Cyber Assets within an identified PSP.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had instituted controls to guard against unauthorized access to the Cyber Assets. The Cyber Assets resided within a physical access-controlled corporate data center; electronic access to the Cyber Assets was limited to IT system administrators. Also, the Cyber Assets were subject to the corporate policy for change management and resided behind a corporate firewall.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to remove the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R6 (SPP2013012841)
During the Compliance Audit, SPP RE determined that URE's change control and configuration management process did not address the replacement and removal of CCA hardware. Additionally, URE did not have a documented process to address disposal of a failed third-party proprietary network monitoring device, nor could it demonstrate that a replacement for the failed device was appropriately implemented.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had evidence to demonstrate that wiping of the failed third-party device had occurred during disposal, and that no harm to its network operations occurred as a result of implementation of the replacement device. Prior to the installation of the new device, the failed device was successfully run on the network for multiple years without any degradation of network operations.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to expand its change control and configuration management process to include third-party proprietary devices.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (SPP2013012842)
During the Compliance Audit, SPP RE determined that URE maintained lists of personnel with authorized cyber and unescorted physical access to CCAs. However, URE's quarterly reviews did not include a review of the specific authorized cyber access rights of personnel, as required by this Standard.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not review the specific access rights on a quarterly basis, it did: i) maintain an access list with specific access rights; ii) review and modify (if necessary) access rights each time the status of an individual on the access list changed; and iii) grant access to URE's CCAs to

only personnel with cybersecurity training and a PRA. URE also conducted quarterly reviews of its access list, which included re-verification of each individual's status, verification of completion of the required annual cybersecurity training, and determination of the status of each individual's PRA. During mitigation, URE confirmed that each affected employee's specific assigned access rights were correct.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to include in its quarterly reviews of access lists specific authorized cyber access rights of URE personnel.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-3a R5 (R5.1 and R5.2) (SPP2013012844)

During the Compliance Audit, SPP RE determined that URE placed a jump box into service. However, URE did not update its documentation to reflect the processes and configurations associated with the device. Additionally, URE removed a virtual private network (VPN) utilized for vendor emergency support, but did not update its ESP network diagram documentation within 90 calendar days of the change.

SPP RE determined that URE had a violation of CIP-005-3a R5.1 and R5.2 for failing to update its documentation related to the jump box, as required, and failing to update its ESP network diagram within 90 days.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE only allows remote access via one jump box device, and the administration of the access model involves a small number of staff. The VPN removal issue was documentation-related.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update its network diagram documentation to reflect the removal of the VPN;

2. retrain affected staff on timely updating network or controls documentation; and

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2 R1 (R1.6) (SPP2013012845)
During the Compliance Audit, SPP RE determined that URE did not consistently follow the visitor control program defined in its physical security plan. URE's manual logs for visitor access into its primary and backup control centers contained multiple instances of illegible personnel escort and visitor names, missing and incomplete information, and information listed in the wrong columns.

SPP RE determined the duration of the violation to be from the date of the first identified log deficiency, through the date of the last identified log deficiency.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. As required by URE's procedure, the visitors at issue were all escorted while inside URE's PSP. Furthermore, video monitoring is enabled at URE's facility. Moreover, URE deploys network monitoring to monitor the up/down state of devices within its environment, thereby enabling early detection of attempted sabotage. Lastly, the discrepancies in the visitor logs were the result of inconsistent recording and did not represent complete failures to identify the entering parties.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop an example of how the manual log should be filled out; and
2. train personnel on how to properly fill out the manual log.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R5 (SPP2013013117)
URE submitted a Self-Report stating that, following a port scan conducted during URE's 2013 CVA, remote terminal unit (RTU) supporting alarms for URE's PSP door monitoring at its back-up facilities ceased to function. URE detected the failure and brought the alarm functions back on-line.

URE supplemented its Self-Report stating that a technician moved a server, which caused a cable to become disconnected from the aforementioned RTU, again resulting in a loss of alarm functionality. The issue was discovered and fixed.

SPP RE determined that URE had a violation of CIP-006-3c R5 for failing to maintain alarm functionality for an access point to the PSP on two instances.

SPP RE determined the duration of the violation to be from the date of the initial RTU alarm failure, through when the RTU alarm functionality was restored following the second failure.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The facilities' physical access points are monitored at all times via closed circuit television, and the access systems continued to authorize access appropriately. Notwithstanding the RTU alarm function failure, the RTU continued to log access, and URE determined that no unauthorized access occurred during the time the alarm function was unavailable.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. reboot the RTU to re-establish alarm functionality following the initial failure;
2. reattach the disconnect cable following the second failure; and
3. implement an alarm to notify personnel when the RTU alarm functionality is down.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of forty-five thousand dollars ($45,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. URE had prior violations of CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, and CIP-009. SPP RE considered some of these prior violations as aggravating factors in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SPP RE considered a neutral factor;

3. URE agreed to: i) restructure its CIP compliance program; ii) hire an additional system administrator; iii) convene a one-day compliance workshop with SPP RE staff; and iv) enhance its EMS to include an asset management system.
4. URE received mitigating credit for self-reporting the following violations: SPP2013012355, SPP2013012356, and SPP2013013117;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations posed minimal or moderate but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of forty-five thousand dollars ($45,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of forty-five thousand dollars ($45,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REMOVED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

October 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Texas Reliability Entity, Inc. (Texas RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Texas RE's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred and six thousand dollars ($106,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012232	CIP-002-1	R2	High/Severe	$106,000
TRE2013012261	CIP-002-1	R3; R3.1; R3.2	High/Severe	
TRE2013012233	CIP-003-1	R4; R4.3	Medium/Severe	
TRE2012011153	CIP-003-1	R5; R5.1; R5.2; R5.3	Lower/Severe	
TRE2012011159	CIP-004-1	R4; R4.1	Lower/Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012235	CIP-005-1	R1; R1.4; R1.6	Medium/ Moderate	$106,000
TRE2012011177	CIP-005-3	R5; R5.2	Lower/Lower	
TRE2013012262	CIP-006-1	R3	Medium/ Moderate	
TRE2013012624	CIP-006-3c	R5	Medium/Severe	
TRE2013012625	CIP-006-3c	R6	Lower/Severe	
TRE2012011178	CIP-007-1	R1; R1.1; R1.2; R1.3	Medium/High	
TRE2013012970	CIP-007-3a	R1; R1.2; R1.3	Medium/Severe	
TRE2013012968	CIP-007-1	R2; R2.1	Medium/Severe	
TRE2012011179	CIP-007-3a	R3; R3.1; R3.2	Lower/Severe	

NERC Violation ID	Standard	Req	VRF/ VSL	Penalty Amount
TRE2013012971	CIP-007-3a	R3; R3.2	Lower/Severe	$106,000
TRE2012010877	CIP-007-1	R4	Medium/Moderate	
TRE2013012972	CIP-007-3a	R4; R4.2	Medium/Severe	
TRE2013012234	CIP-007-1	R5; R5.1; R5.2; R5.3.3	Medium/Severe	
TRE2012011180	CIP-007-2a	R9	Lower/High	
TRE2012011181	CIP-008-3	R1; R1.2	Lower/Moderate	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

OVERVIEW

This Settlement Agreement resolves 20 CIP violations discovered throughout 2012 and 2013. The violations were discovered through a series of Self-Certifications, Self-Reports, and a Compliance Audit.

CIP-002-1 R2 (TRE2013012232)

URE submitted a Self-Report stating that it was in violation of CIP-002-1 R2. Specifically, URE reported that it discovered errors in its list of identified Critical Assets determined through an annual application of its risk-based assessment methodology. URE discovered that, in several instances, it erroneously included or omitted substations on its Critical Assets list. The cause was an oversight by URE when transcribing Critical Asset information from its various maps and lists to the final Critical Assets list.

Texas RE determined that URE had a violation of CIP-002-1 R2 for failing to update its Critical Asset lists accurately after applying its annual risk-based assessment methodology.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed preparation of its Critical Assets list.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE applied its annual risk-based assessment methodology. Although URE did not include certain Critical Assets on its official Critical Assets list, URE correctly identified its Critical Assets on maps and other lists as Critical Assets and protected them as such. URE managed all station-based Cyber Assets with the same safeguards, using the same procedures, processes, security measures, tools, and protocols.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. finalize its new procedure containing its methodology for identifying Critical Assets and updating CCAs and Technical Feasibility Exceptions (TFEs);
2. conduct training on the new procedure for all stakeholders involved in the annual risk-based assessment process;
3. post the new procedure to its compliance database to facilitate access by appropriate personnel, and send an email to affected personnel in charge of implementing the new procedure; and
4. complete development of the annual Critical Asset list applying the new procedure.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-002-1 R3 (R3.1, R3.2) (TRE2013012261)

URE submitted a Self-Report stating that it was in violation of CIP-002-1 R3. Specifically, URE reported that it discovered errors in its CCA lists for several years. These errors consisted of the following: (i) failure to identify switches with routable protocols that were connected to two backup inter-control center protocol (ICCP) devices as CCAs (this occurred after an Electronic Security Perimeter (ESP)

reconfiguration was completed); (ii) multiple instances where stations and their associated CCAs were incorrectly included on the CCA list; and (iii) multiple instances where stations and their associated CCAs were omitted from the CCA list.

Texas RE determined that URE had a violation of CIP-002-1 R3 for failing to develop a complete and accurate list of associated CCAs essential to the operation of Critical Assets.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed development of the annual CCA list.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to document the list accurately, the CCAs that were left off the CCA list were within secured ESPs and afforded the protections included in CIP-003-1 through CIP-009-1. The CCAs were protected by URE's firewalls and by URE's intrusion prevention system. This system monitored and provided alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and investigated. URE's core network, which included all primary CCAs, was physically located in a secure room within a secure facility that was monitored at all times. Additionally, URE managed all relevant Cyber Assets with the same safeguards, procedures, processes, security measures, tools, and protocols.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. disconnect the switches and logically reconfigure them back to their original location;
2. update the CCA and ESP lists to reflect the current ESP configuration;
3. implement enhancements to the change management procedure to minimize the potential for recurrence;
4. conduct a thorough review of the devices to ensure all relevant CCAs have been identified and documented on the CCA and ESP lists. URE also developed a new procedure to document the process of completing this review on a periodic basis to ensure the ESP list is accurate;
5. train the appropriate personnel on the enhanced change management procedure and on the new procedure for establishing and maintaining ESPs;
6. implement these new procedures and post them to its compliance database to facilitate access by appropriate personnel;

7. create a new methodology for identifying CAs and updated CCAs and TFEs to include a more robust process of inclusion, reviews, and controls to help ensure accuracy of its CCA list;
8. conduct training on this new methodology with all stakeholders involved in the annual risk-based assessment process;
9. implement this new methodology and post it to its compliance database to facilitate access by appropriate personnel; and
10. complete development of the annual CCA list using the new methodology.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R4 (R4.3) (TRE2013012233)

URE submitted a Self-Report to Texas RE stating that it was in violation of CIP-003 R4. URE failed to conduct and document all annual assessments of its adherence to its CCA information protection program for two years. Specifically, URE conducted annual adherence assessments for information related to one group, but it did not document the assessments. URE failed to conduct annual adherence assessments for information related to a different URE group.

Texas RE determined that URE had a violation of CIP-003-1 R4 for failing to conduct and document all annual assessments of its adherence to its CCA protection program.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its review of its information protection program, implemented enhancements, and posted the new program documents to a location accessible by appropriate personnel.

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by failing to conduct certain annual adherence assessments of its information protection program, URE failed to have sufficient security management controls in place, and sensitive information related to CCAs could have been compromised. However, although URE did not properly document all aspects of two annual assessments, URE did control access to certain protected information and conducted reviews accordingly. Further, URE's data custodians were appropriately controlling access to documents protected under URE's information protection program.

URE's Mitigation Plan (TREMIT009150) to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a thorough evaluation of its information protection program and create an action plan to identify enhancements;
2. enhance its program documents to clarify and reinforce the requirements related to CIP-003;
3. complete training on the enhanced program documents with personnel responsible for managing protected information; and
4. implement the enhanced program and post associated documents to its compliance database to facilitate access by appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R5 (R5.1, R5.2, R5.3) (TRE2012011153)

URE submitted a Self-Certification stating that it was in violation of CIP-003-1 R5. URE subsequently submitted a more detailed Self-Report.

URE stated that it did not timely update the personnel list for those responsible for authorizing access to protected CCA information. Specifically, URE failed to remove a former employee who left the company from its data custodian list. In addition, URE did not conduct an annual review of access privileges to a particular document management site to confirm that access privileges were correct and that they corresponded with URE's needs and appropriate personnel roles and responsibilities. Moreover, URE did not at least annually assess and document the processes for controlling access privileges to protected information on that same site. URE also reported that it discovered several instances where documents designated as confidential or restricted were attached as documentation from URE's change management system. As a result, any URE or contractor employee who had access to the system could view those documents.

Texas RE determined that URE had a violation of CIP-003-1 R5 for failing to document and implement a program for managing access to protected CCA information that met the requirements of the Standard.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the date URE conducted an annual review of its processes for controlling access privileges to protected information.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/Physical Security Perimeter (PSP) access authentication.

With respect to the document management site, URE confirmed that the site had the appropriate site and document level controls and was managed to ensure controlled access to protected information.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. revise its information protection program to reflect the appropriate data custodians, post the program to its compliance database to facilitate access by appropriate personnel, and send an email communication to applicable personnel informing them that the revised program was implemented and in effect;
2. assign a new data custodian to the document management site, who implemented a process to conduct quarterly reviews of the access privileges to the site;
3. conduct training on the requirements of the revised program with all data custodians and conduct an annual review;
4. redesign the change management system to ensure only those individuals with approved access privileges to protected information can access/view change requests that include protected information;
5. conduct an end-to-end review of the program to identify opportunities and implement enhancements;
6. develop and implement processes for annual program adherence assessment;
7. design and implement an enhanced periodic access review process with centralized documentation maintained in the compliance database;

8. document access privileges criteria and processes for the document management platform, the change management system, the password site, the engineering project software, and the compliance database;
9. enhance the annual review meeting conducted with all data custodians;
10. establish periodic operational and corporate level controls to ensure implementation and adherence to the program; and
11. develop a cross-functional training program, training materials, and schedule required to implement the enhanced process and procedure improvements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (TRE2012011159)

URE submitted a Self-Certification stating that it was in violation of CIP-004-1 R4. URE subsequently submitted a more detailed Self-Report. For CCAs administered by one URE team, URE reviewed a list of personnel who had access to an application that is run on most CCAs, instead of reviewing a list of personnel who had access to the CCAs themselves.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the date URE amended its documentation to correct annual review processes and performed a review to verify the documentation changes.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, intrusion prevention, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/PSP access authentication.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a thorough review of cyber access rights for each individual account on the CCAs in the ESPs administered by the relevant team and update the access authorization list to reflect the current state of CCA access;

2. develop and implement a new process for tracking and reviewing individual account access on CCAs;
3. conduct quarterly reviews of cyber access rights of each user account on each CCA in the ESPs administered by the relevant team and make timely access adjustments;
4. continue access review and associated access adjustments based on daily URE personnel employment status change reports, including review of access for personnel with cyber access to individual accounts on CCAs in the ESPs administered by the relevant team;
5. continue access review and associated access adjustments based on proactive monitoring and communication of contract services personnel employment status, including review of access for personnel with cyber access to individual accounts on CCAs in the ESPs administered by the relevant team;
6. document formally and communicate the new process to affected employees and post the new process and procedure; and
7. identify and train the URE employees within the relevant team who will act as primary and secondary backups for the access review process.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R1 (R1.4, R1.6) (TRE2013012235)

URE submitted a Self-Report stating that it was in violation of CIP-005 R1. URE did not appropriately identify and document five non-critical Cyber Assets in the ESP. Specifically, URE failed to include on an ESP list two non-critical Cyber Assets that connected to two devices within the ESP. URE failed to include one server on any of the ESP lists generated for a period of approximately two years. Lastly, URE listed two servers as CCAs on an ESP list that was generated on a certain date, but it failed to include the servers on any subsequent lists until almost a year later.

Texas RE determined that URE had a violation of CIP-005-1 R1 for failing to identify and document five non-critical Cyber Assets in the ESP.

Texas RE determined the duration of the violation to be from the date one of the servers was not included on the ESP list through when URE updated the ESP documentation to reflect the presence of the non-critical Cyber Assets within the ESP.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it failed to include the five devices on its ESP lists, URE provided the required protections to the devices. The servers should have been classified as non-critical Cyber Assets, as they had never been moved from testing into full production. Lastly, the devices represented less than 5% of all devices protected within ESPs.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. install a network scanning tool that enables URE to conduct total system scans to monitor all ports and devices;
2. complete its new procedure to institute more stringent controls and reviews on URE's ESPs and documentation processes;
3. train the relevant team on the new procedure;
4. perform a scan of the complete ESP;
5. update ESP documentation to reflect the presence of non-critical Cyber Assets; and
6. post and implement the new procedure.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-005-3 R5 (R5.2) (TRE2012011177)

URE submitted a Self-Certification stating that it was in violation of CIP-005-3 R5. URE subsequently submitted a more detailed Self-Report.

URE reported that it failed to update documentation to reflect the modification of the network or controls within 90 calendar days of the change. Specifically, URE moved two Critical Assets from one ESP to another ESP and failed to document the change within 90 days. Further, when URE created the new documentation, it contained errors.

Texas RE determined that URE had a violation of CIP-005-3 R5 for failing to update the documentation to reflect the modification of the network or controls within 90 calendar days.

Texas RE determined the duration of the violation to be from 90 days after when URE moved the two Critical Assets from one ESP to another ESP through when URE updated its documentation to reflect the correct location of the Critical Assets.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The Critical Assets at issue were protected by URE's ESPs, and they comprised a small percentage of URE's total Critical Assets. Further, URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incident detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. Lastly, the affected devices were physically located in a secure room within a secure facility that was monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. relocate the devices from the new ESP back to the original ESP;
2. update the ESP and CCA documentation;
3. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of the violation and develop other related improvements;
4. develop and document a procedure for establishing, reviewing, and updating ESPs;
5. enhance the procedure for identifying, reviewing, and updating CCAs; and
6. develop a cross-functional training program, training materials, and schedule required to implement the enhanced process and procedure improvements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R3 (TRE2013012262)

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R3. Specifically, although appropriately equipped with card reader access restrictions managed through URE's access management and logging system, URE was not monitoring access to one of its PSP doors. The door

was left off the list for URE's security management contractor. Because the door was not being monitored by the security contractor, URE was not immediately reviewing unauthorized access attempts to a PSP for the door.

Texas RE determined that URE had a violation of CIP-006-1 R3 for failing to implement technical and procedural controls for monitoring physical access at all access points to the PSP at all times.

Texas RE determined the duration of the violation to be from the date the standard became mandatory and enforceable on URE through the date URE transferred access monitoring from the contractor to URE.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The door was located in a secure URE facility that was staffed at all times. Further, the door was appropriately equipped with card reader access restrictions managed through URE's access management and logging system.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. enhance its physical security plan based on results of URE's annual procedure review;
2. update the plan to reflect the current security measures as observed through a walk-through of the PSP;
3. provide training to appropriate personnel on the enhanced plan;
4. post and implement the enhanced plan; and
5. bring PSP access monitoring fully under URE's supervision.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R5 (TRE2013012624)

URE submitted a Self-Report stating that it was in violation of CIP-006-3c R5. URE explained that it replaced an existing air conditioning unit in service in a PSP. A panel was removed from the wall of the PSP and from the wall of the adjacent mechanical room to provide venting for the temporary air

conditioning unit. The removal of those panels created a space in the wall, thereby creating a temporary access point to the PSP. Security monitoring equipment was in place and was monitoring and logging access to the temporary access point. However, alarming had been disabled.

Several hours later, a URE employee investigated and determined that alarming was not in place for the temporary access point, and requested that it be re-initiated. Alarming was re-initiated a few minutes later.

Texas RE determined that URE had a violation of CIP-006-3c R5 for failing to implement its technical and procedural controls for monitoring physical access at all access points to the PSP at all times.

Texas RE determined the duration of the violation to be for several hours, from the time the temporary access point was created until alarming was re-initiated.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The temporary access point was located within a secured and monitored building protected by a secured, fenced yard. Both the building and the yard were equipped with key card access control, and the area was staffed at all times. Security monitoring equipment was in place and was monitoring and logging access to the temporary access point. However, the alarming was off for the period of the violation. Logging of the temporary access point indicated that there was no activity in the mechanical room within the period that alarming was disabled.

URE's Mitigation Plan to address this violation was submitted to Texas RE.

URE's Mitigation Plan required URE to:

1. re-initiate alarming for the temporary access point;
2. install permanent grating over the penetration in the PSP to eliminate the possibility of recurrence; and
3. distribute, to managers and supervisors at the PSP, URE's procedure specifying the controls used to manage access to PSPs.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R6 (TRE2013012625)

URE submitted a Self-Report to Texas RE stating that it was in violation of CIP-006-3c R6. URE failed to ensure that an air conditioning contractor working in a PSP signed URE's access log as required by URE's physical security plan. The contractor was appropriately escorted during his presence in the PSP.

Texas RE determined that URE had a violation of CIP-006-3c R6 for failing to implement its technical and procedural mechanisms for logging physical entry at all access points to the PSP.

Texas RE determined the duration of the violation to be for several hours on the date the contractor worked in the PSP without having signed the access log.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The contractor was appropriately escorted at all times while inside the PSP. Further, the PSP was within a secured and monitored building that was within a secured, fenced yard. Both the building and the yard were equipped with key card access control, and the area was staffed at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE.

URE's Mitigation Plan required URE to:

1. provide specific counseling relating to CIP physical security requirements and URE's physical security plan to the employee who escorted the contractor within the PSP but failed to ensure the contractor signed the access log;
2. reinforce the applicable requirements related to CIP physical security and URE's physical security plan with each member of staff leadership at the PSP, including all managers and supervisors; and
3. require its managers and supervisors at the PSP to review and acknowledge the procedure that specifies the controls used to manage access to PSPs.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (R1.1, R1.2, R1.3) (TRE2012011178)

URE submitted a Self-Certification stating that it was in violation of CIP-007-1 R1. URE subsequently submitted a more detailed Self-Report. URE reported that it failed to complete documentation that it performed testing, prior to making changes to existing Cyber Assets, in a manner that reflects the production environment. URE also reported that it failed to implement its procedure effectively to ensure personnel understood the need to document that testing was performed in a manner that reflects the production environment and to document test results in URE's change management system.

Texas RE determined that URE had a violation of CIP-007-1 R1 for failing to implement effectively its test procedures to ensure that changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE did not properly train its personnel. Failure to document that significant changes to the Cyber Assets within the ESP were tested in a manner that reflects the production environment and to document test results could have introduced vulnerabilities or modified existing cybersecurity controls. However, although not consistently documented, significant changes to Cyber Assets within the ESP were tested in a manner that reflects the production environment. All CCAs were protected by URE's firewalls and its intrusion prevention system, which was monitoring and providing alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and investigated. Further, URE's primary CCAs were physically located in a secure room within a secure URE facility that is monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. conduct a review of URE's change management procedure and make enhancements to the testing plan included in the procedure;
2. conduct training on the enhanced procedure for the members of the team who perform testing of changes to Cyber Assets within the ESPs that they administer. The training was designed to ensure that personnel understand the need to document that testing is performed in a manner

that reflects the production environment and that all test results must be documented in URE's change management system;

3. implement and post the updated procedure to a database to facilitate access by relevant personnel; and
4. establish a team to address the causes of this violation and to develop other related process improvements, as appropriate.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-3a R1 (R1.2, R1.3) (TRE2013012970)

During the Compliance Audit, Texas RE determined that URE was in violation of CIP-007-3a R1. URE did not document the test results for a number of change requests for significant changes as required by URE's change control and configuration management procedure. Texas RE determined certain change requests for significant changes to Cyber Assets within an ESP did not contain evidence indicating testing processes were followed or testing results were documented as required by that procedure.

Texas RE determined that URE had a violation of CIP-007-3a R1 for failing to document that testing is performed in a manner that reflects the production environment and for failing to document test results.

Texas RE determined the duration of the violation to be from the date documentation was discovered missing through when URE amended its procedure to provide more clarity on the necessary steps for testing and documentation.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did document change requests completed for significant changes to Cyber Assets within ESPs, but did not retain documentation related to testing processes and results prior to the change requests being completed. Further, testing of significant changes is done within URE's development environment and prior to application within ESPs.

To mitigate this violation, URE:[4]

1. conducted training on the change management test plan;

[4] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012970.

2. updated its process to provide more clarity on the necessary steps for testing and documentation, and created a change approval board as a new control to manage and monitor the completion and documentation of changes;
3. reviewed results of the Compliance Audit and reinforced focus on compliance in meeting of the relevant URE team;
4. added information technology operational expertise to the relevant URE team as part of a phased approach to organizational realignment;
5. developed change request documentation guide providing more clarity on impact assessment, work plan, test plan, and test results documentation;
6. established and implemented enhanced change request approval and review processes;
7. reviewed all open change requests for required documentation prior to close-out for significant changes implemented after a certain date;
8. enhanced URE's change management and responsibilities matrix procedures to clarify individual expectations and accountabilities;
9. trained relevant personnel on procedural enhancements; and
10. implemented and posted enhanced procedures.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R2 (R2.1) (TRE2013012968)

During the Compliance Audit, Texas RE discovered that URE failed to disable ports and services that were not required for normal and emergency operations. Texas RE enforcement determined that URE opened two ports and services on a single device to support troubleshooting and testing, but it inadvertently failed to turn them off when introducing the device to the production environment.

Texas RE determined that URE had a violation of CIP-007-1 R2 for failing to implement its process to ensure that only those ports and services required for normal and emergency operations are enabled.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE removed the ports and services.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The ports at issue were not required for normal or emergency operations but

were enabled for testing purposes. The ports represented point-to-point connections between Cyber Assets, and other Cyber Assets outside the specific environment could not access them.

To mitigate this violation, URE:[5]

1. removed the ports and services that were inadvertently left open; and
2. strengthened its approach to preparing devices to enter the production environment.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-3a R3 (R3.1, R3.2) (TRE2012011179)

URE submitted a Self-Certification stating that it was in violation of CIP-007-3a R3. URE subsequently submitted a more detailed Self-Report. URE stated that, in two instances, it failed to assess, and therefore document, security patches for two types of servers.

Texas RE determined that URE had a violation of CIP-007-3a R3 for failing to assess security patches for applicability within 30 calendar days of availability.

Texas RE determined the duration of the violation to be from the date when URE first failed to address a patch through when URE addressed the outstanding patches.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. These devices were located in a secure room within a secure URE facility that was monitored at all times.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop and implement a biweekly patch remediation process for the devices;

[5] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012968.

2. develop and implement a new security patch management process; also, communicate the process to the relevant team to ensure a common understanding of security patch management as it applies to the servers;
3. evaluate and implement enhancements to the security patch management section of the change management procedure;
4. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of noncompliance and to develop other related improvements;
5. develop and implement a security patch management assessment desktop procedure to facilitate a consistent approach and consistent documentation;
6. develop a cross-functional training program, training materials, and schedule to implement enhanced process and procedure improvements; and
7. establish periodic operational and corporate level controls to ensure security patch management assessment and documentation is conducted and documented in accordance with URE procedures.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-3a R3 (R3.2) (TRE2013012971)

During the Compliance Audit, Texas RE discovered that URE was in violation of CIP-007-3a R3. Specifically, URE installed eight security patches on a server, but it did not complete documentation of the implementation of the patches.

Texas RE determined that URE had a violation of CIP-007-3a R3 for failing to document the implementation of security patches.

Texas RE determined the duration of the violation to be from the date URE installed patches but did not complete documentation of the implementation through when URE documented its implementation of the patches.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although its test plan documentation was deficient, Texas RE determined that URE's servers were shown to have security patches applied. URE testing personnel verified and signed

off on test plan results for cybersecurity controls modification. In addition, URE uses multiple layers of defense, including the use of intrusion prevention systems, firewalls, and network segmentation. URE has strong defenses for external cyber-attacks, and internally there is a substantial effort to reduce risk for internal attacks, viruses, and malware.

To mitigate this violation, URE:[6]

1. documented its implementation of security patches;
2. amended its patch management procedures;
3. reviewed Compliance Audit results and reinforced focus on compliance in the department; and
4. reassigned information technology operational expertise to the relevant team as part of a phased approach to organizational realignment.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R4 (TRE2012010877)

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R4. URE did not have antivirus and malware protection software installed on six devices and three servers. These nine devices are Cyber Assets within the ESP.

Texas RE determined that URE had a violation of CIP-007-1 R4 for failing to have antivirus and malware prevention software installed on nine Cyber Assets within the ESP.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed installing antivirus and malware prevention software on the nine affected devices.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a robust system that included a layered approach to protecting its Cyber Assets. This approach included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and ESP/PSP access authentication. URE's firewalls and intrusion prevention system monitored and provided alerts of any unknown communication types within the ESP. Real-time alerts were automatically raised and

[6] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012971.

investigated. In addition, the affected devices were physically located in a secure room within a secure URE facility that was monitored at all times.

To mitigate this violation, URE:[7]

1. installed antivirus and malware prevention software on the affected devices, confirmed the installation of the software on those devices, and confirmed that antivirus and malware prevention software was installed on all other Cyber Assets within URE's ESP;
2. reviewed the antivirus and malware protection procedure and the change management procedure, developed enhancements for those procedures, and developed related desktop procedures;
3. developed and implemented new training for employees responsible for tasks in the new and enhanced procedures;
4. conducted annual NERC compliance training for all employees responsible for implementing and sustaining compliance with Reliability Standards;
5. conducted quarterly CIP awareness sessions to review highlights of industry activity and enhancements in program (ongoing); and
6. implemented a monthly process in which signature update files are validated on all Cyber Assets in the ESPs administered by the relevant team. The process includes a step for a second team member to review and validate the results.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-3a R4 (R4.2) (TRE2013012972)

During the Compliance Audit, Texas RE discovered that URE did not implement its process for updating antivirus signatures for three of its servers. These three servers lost their client relationship with the managing server to receive virus definition updates.

Texas RE determined that URE had a violation of CIP-007-3a R4 for failing to implement its process for the update of antivirus and malware prevention signatures.

[7] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2012010877.

Texas RE determined the duration of the violation to be from the date when the first of the three servers lost its client connection to the antivirus update server through the date when the last of the three servers' client connection was restored and antivirus signatures were updated.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. While these servers were not protected with the latest antivirus and malware prevention signatures during the specified period, URE used multiple layers of defense for compensating measures. URE has strong defenses for external cyber-attacks, and internally there is a substantial effort to reduce risk for internal attacks, viruses, and malware.

To mitigate this violation, URE:[8]

1. updated signatures on the three servers; and
2. updated and implemented its antivirus and malware prevention procedures.

URE submitted a Mitigation Activity Completion Affidavit stating that the above mitigating activities were completed. Texas RE verified the completion of URE's mitigating activities.

CIP-007-1 R5 (R5.1, R5.2, R5.3.3) (TRE2013012234)

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R5 in several instances. URE's shared and default account access list did not contain a complete listing of all shared and default accounts and associated access privileges for the Cyber Assets in the ESPs. In addition, URE did not change passwords to all shared and default accounts for the Cyber Assets in the ESPs on an annual basis. This issue affected Cyber Assets administered by a specific URE team.

Texas RE determined that URE had a violation of CIP-007-1 R5 for failing to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

Texas RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE created a comprehensive user access list for shared and default accounts and changed all shared and default account passwords.

Texas RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure could have resulted in unauthorized access

[8] Texas RE did not require URE to submit a formal Mitigation Plan for TRE2013012972.

to URE's Cyber Assets and put URE's system at risk. Inadequate password requirements and failure to ensure password changes could have increased the risk of unauthorized individuals with malicious intent gaining access to URE's Cyber Assets. A complete listing of all shared and default accounts and associated access privileges for the Cyber Assets in the ESPs had never been created. The identified list of default accounts provided as part of the cyber vulnerability assessment was incomplete. The risk was further increased because the list was missing almost half of accounts. The accounts that were identified as missing from the list included default accounts with strong controls and disabled accounts.

However, the risk was mitigated by the following factors. URE limited access to the affected Cyber Assets to a small group of employees and contractors whose access rights were closely monitored by the team's manager. The Cyber Assets themselves were located in protected ESPs behind secure PSPs. Cyber and physical access rights to CCAs in the ESP were being monitored and managed through timely employment status alerts and associated timely access revocation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. create a new, comprehensive user access list for shared and default accounts;
2. change passwords on all Cyber Assets and CCAs with shared/default accounts in the ESPs administered by the relevant team;
3. update its responsibilities matrix procedure to help ensure the requirements of CIP-007 R5 are met;
4. train appropriate personnel on the updated procedure; and
5. implement the updated procedure and post it to the compliance database to facilitate access by appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-007-2a R9 (TRE2012011180)

URE submitted a Self-Certification stating that it was in violation of CIP-007-2a R9. URE subsequently submitted a more detailed Self-Report stating that it failed to update its change management

procedure within 30 calendar days of a change being completed. Specifically, URE implemented its change management system on one date, but it did not update a section of its procedure until over a year later.

Texas RE determined that URE had a violation of CIP-007-2a R9 for failing to document changes resulting from modifications to systems or controls within 30 calendar days of the change being completed.

Texas RE determined the duration of the violation to be from the date by which URE should have amended its documentation through when URE amended its documentation.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did implement the new system and documented the implementation in its procedure document. However, URE failed to update an additional section of its procedure, the disposal and redeployment section, to reflect the use of the change management system. There were no disposals or redeployments of Cyber Assets administered by the relevant team during the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update its change management procedure to reflect implementation of URE's change management system, post the procedure to its compliance database to facilitate access by appropriate personnel, implement the procedure, and issue an email communication to applicable personnel;
2. conduct training on the revised procedure with all applicable personnel;
3. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of the noncompliance and to develop other related improvements;
4. review the revised procedure and associated training for accuracy and completeness; and
5. establish periodic operational and corporate level controls to ensure documentation updates.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

CIP-008-3 R1 (R1.2) (TRE2012011181)

URE submitted a Self-Certification stating that it was in violation of CIP-008-3 R1. URE subsequently submitted a more detailed Self-Report. URE reported that its Cyber Security Incident response plan did not reflect all appropriate personnel updates. Specifically, the text of the plan was not revised to reflect the position changes that were included on URE's list of people to be contacted in the event of an incident (this list was attached to the plan). URE does include a process for updating its plan within 30 calendar days, but URE failed to update contact changes within 30 days according to its process.

Texas RE determined that URE had a violation of CIP-008-3 R1 for failing to reflect personnel updates in its Cyber Security Incident response plan.

Texas RE determined the duration of the violation to be from when the Cyber Security Incident response plan did not reflect all personnel updates through when URE updated the plan to reflect all appropriate personnel updates.

Texas RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In the event of an incident, the relevant manager would have notified the personnel on the contact list who would have communicated with the appropriate personnel on their respective teams. Additionally, the contact information was correct for most of the people on the incident response team. Lastly, URE did not experience an incident requiring the use of the contacts list during the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to Texas RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update the Cyber Security Incident response plan contact list, post the plan to the compliance database to facilitate access by applicable personnel, implement the plan, and issue an email to appropriate personnel;
2. conduct training on the revised plan with all applicable personnel;
3. update the plan's investigation requirements, post the plan to the compliance database, and issue an email to applicable personnel;
4. conduct training on the revised plan with all applicable personnel;

5. establish a process improvement team to develop and document enhanced processes and procedures to address the causes of noncompliance and develop other related improvements as appropriate; and
6. review the revised plan and associated training to evaluate potential enhancements.

URE certified that the above Mitigation Plan requirements were completed.

Texas RE verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, Texas RE has assessed a penalty of one hundred and six thousand dollars ($106,000) for the referenced violations. In reaching this determination, Texas RE considered the following factors:

1. Texas RE did not consider URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations which Texas RE considered a mitigating factor;
3. URE self-reported several of the violations;
4. in addition to the mitigating activities described above, URE has undertaken actions beyond those necessary to come into compliance with the Standards. URE continues to implement its self-assessment program, making several enhancements;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations posed a minimal or moderate risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, Texas RE determined that, in this instance, the penalty amount of one hundred and six thousand dollars ($106,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the factors considered by Texas RE, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and six thousand dollars ($106,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REMOVED FROM THIS PUBLIC VERSION

[9] *See* 18 C.F.R. § 39.7(d)(4).

[10] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Derrick Davis* Director, Enforcement, Reliability Standards & Registration Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4923 (512) 233-2233 – facsimile derrick.davis@texasre.org	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Rachel Coyne* Enforcement Analyst, Sr. Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4956 (512) 233-2233 – facsimile rachel.coyne@texasre.org

Abby Fellinger* Enforcement Analyst Texas Reliability Entity, Inc. 805 Las Cimas Parkway Suite 200 Austin, TX 78746 (512) 583-4927 (512) 233-2233 – facsimile abby.fellinger@texasre.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Texas Reliability Entity, Inc.

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

November 25, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entities, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), and Unidentified Registered Entity 3 (URE3), (collectively, the UREs), NERC Registry ID# NCRXXXXX , NCRXXXXX, and NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Midwest Reliability Organization (MRO), on behalf of itself, Southwest Power Pool Regional Entity (SPP RE), and Western Electricity Coordinating Council (WECC), and the UREs have entered into a Settlement Agreement to resolve all outstanding issues arising from MRO's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the UREs do not contest the violations and have agreed to the assessed penalty of one hundred and fifty thousand dollars ($150,000) in addition

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
MRO2012009882	CIP-003-2	R5; R5.1.1; R5.1.2; R5.2; R5.3	Lower/ Severe	The UREs	$150,000[4]
MRO201100289	CIP-003-1	R6	Lower/ Severe	URE1, URE3	
MRO201100323	CIP-004-2	R3; R3.1; R3.2	Medium/ High	URE1, URE3	
MRO201100322	CIP-004-1	R4; R4.1	Lower/ High	URE1	

[4] MRO shall divide the penalty amount in three parts based on the relative net energy for load of each Regional Entity.

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
MRO2012010698	CIP-004-3	R4; R4.1; R4.2	Lower/ High	The UREs	$150,000
MRO201100287	CIP-005-1	R1; R1.5	Medium/ Severe	The UREs	
MRO2012009900	CIP-005-1	R1; R1.5; R1.6	Medium/ Severe	The UREs	
MRO201100288	CIP-005-1	R5; R5.1; R5.2	Lower/ Severe	URE1, URE3	
MRO201100325	CIP-006-1	R1; R1.2; R1.3; R1.7	Medium/ Severe	URE1	
MRO2012009899	CIP-006-1	R1; R1.8	Lower/ Severe	The UREs	
MRO2012011501	CIP-006-1	R1; R1.8	Lower/ Severe	The UREs	
SPP2012010242	CIP-006-1	R1; R1.8	Lower/ Severe	The UREs	
MRO201100290	CIP-006-3a	R2; R2.1; R2.2	Medium/ Severe	The UREs	
MRO2012010967	CIP-006-3c	R4	Medium/ Severe	URE1	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Applicable Function(s)	Total Penalty
MRO2012010966	CIP-006-3c	R6	Lower/ Severe	URE1	$150,000
SPP2012010241	CIP-007-1	R3	Lower/ Severe	URE1 URE2	
MRO201000232	CIP-007-1	R5; R5.2.3	Medium/ Severe	URE1, URE3	
MRO2012009992	CIP-007-1	R5; R5.3.1; R5.3.2; R5.3.3	Medium/ Severe	The UREs	
MRO201100292	CIP-007-1	R7; R7.1; R7.2	Lower/ Severe	URE1, URE3	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

The UREs notified MRO that they had identified several compliance concerns and would be conducting a comprehensive review of their CIP compliance program. The UREs submitted multiple Self-Reports to MRO, SPP RE, and WECC. Also during this time, MRO conducted a CIP Compliance Audit of URE1, while SPP RE and WECC jointly conducted a CIP Compliance Audit of URE2 and URE3. MRO reports that, throughout the process of conducting their comprehensive review, the UREs have been actively communicating and meeting with staff from MRO, SPP RE, and WECC.

This Settlement Agreement includes 19 violations:

1. eight violations processed by MRO on behalf of MRO, SPP RE, and WECC;
2. five violations processed by MRO on behalf of MRO and WECC;
3. four violations in the MRO region only; and
4. two violations processed by SPP RE on behalf of MRO, SPP RE, and WECC.

CIP-003-2 R5 (R5.1.1, R5.1.2, R5.2, R5.3) (MRO2012009882)

URE1 submitted a Self-Certification to MRO stating it was in violation of CIP-003 R5. URE2 and URE3 also reported noncompliance with the same standard and requirement to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to implement their program for managing access to protected Critical Cyber Asset (CCA) information.

The UREs conducted a survey to identify CIP information, determine whether the information was classified appropriately, and determine whether or not it was protected in compliance with CIP requirements and the UREs' CIP information protection program. The survey results identified that several CIP information repositories (electronic file locations) used to store CIP protected information did not have all the necessary access controls in place.

The UREs' CIP information protection program required that all CIP protected information be stored in a specified folder structure within a repository for which the required controls were in place. The UREs' CIP protected information was also being stored in other repositories that did not have all required access controls in place. Additionally, the UREs identified nearly 10% of users with incorrect access privileges to protected information.

MRO determined that the UREs had a violation of CIP-003-2 R5 for failing to implement their program for managing access to protected CCA information.

MRO determined the duration of the violation to be from the first date CIP protected information was found to reside in a repository without the required access controls through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). The UREs control multiple BPS facilities. The violation continued for two years and involved nearly 10% of all user accounts and several unauthorized repositories. Examples of repositories that were not subject to the access controls specified in CIP-003 R5 included network drives, internal document sharing sites, and other internal non-approved document management systems accessible by multiple individuals that were not part of the UREs' CIP program. Examples of protected documents stored in the unapproved repositories included CIP policies and procedures, physical access control system programming information, security plans and drawings, Technical Feasibility Exception (TFE) working documents, and shared password change evidence. Further, the UREs overall information protection program was found to be inadequate.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. revise the CIP access control program to include the CIP-003 R5 requirements necessary to secure and protect CIP information repositories;
2. train all CIP information repository owners and administrative support staff on the revised CIP access control program;
3. require each repository owner and administrative support staff to document the process and procedures for controlling access to his or her respective repository or security group;
4. require each repository owner and administrative support staff to review the user access privileges for his or her respective repository or security group to confirm that they are correct and that they correspond with the appropriate business need-to-know requirement;
5. remove access for any individuals that no longer required access; and
6. identify CIP information repositories that store CIP protected information and add the repository owners, titles, and name of the repository for which they approve access to the designated approver personnel list.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-003-1 R6 (MRO201100289)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-003-1 R6. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

Specifically, URE1 and URE3 (collectively, the UREs) failed to follow their substation change control process to ensure all CCAs were subjected to the change control and configuration management program, for both changes to existing CCAs and the addition of new devices into existing Critical Asset environments. This failure resulted in the inconsistent identification and tracking of new CCAs and an inconsistent application of the UREs' change control and configuration management program.

The Self-Report was the result of an internal inventory conducted by the UREs of Cyber Assets within the Electronic Security Perimeter (ESP) of BPS substations. The internal assessment identified discrepancies between CCAs contained on lists maintained by URE1 and URE3 and those deployed in the field. After further review, the UREs determined that certain BPS substation CCAs commissioned

or decommissioned after a certain date had not been handled in a manner consistent with the UREs' substation change control and configuration management process.

The UREs identified multiple instances of changes to substation CCAs subject to CIP-003-1 R6 where they failed to follow their process for change management. Of the total number of changes, most involved the addition of new CCAs to a substation. The UREs failed to follow the required configuration management and change control process and appropriately update documentation. These CCAs included primary and secondary line relaying, bus differential relaying, and breaker failure relaying at substations. The UREs also failed to follow their change management process for CCAs, including substation protective relays that underwent modification or retirement.

This violation was also the root cause of additional self-reported violations of CIP-005-1 R5 (MRO201100288) and CIP-007-1 R7 (MRO201100292).

MRO determined that the UREs had a violation of CIP-003-1 R6 for failing to follow their substation change control process to that ensure all CCAs were subjected to their change control and configuration management program.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the UREs' newly-added CCAs were not properly documented upon installation and not properly included in the UREs' CIP compliance program. Therefore, they were not ensured protection under the CIP Reliability Standards. Without proper protections, these CCAs were vulnerable and could potentially have been exploited. The CCAs were located at critical high-voltage substations and Interconnection Reliability Operating Limit flow gates. Further, the duration of the violation was over two years.

However, several factors mitigated the risk posed by the violation. The change control issue was limited. Although the changes did not follow the additional requirements for CCAs, the UREs followed their standard testing, checkout, and commissioning process, which provided substantial security controls. None of the changes were related to the electronic access management system, which provided primary remote access security control for the substations affected by the violation. The process weakness that allowed this violation was not present for this system. Lastly, the UREs did not experience any issues with their energy management systems (EMS) during the pendency of the violation.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the pre-commissioning checklist;
3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement it by starting use of the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;
9. inform MRO of status of contacting the other utilities; and
10. execute an additional action plan to augment the substation change control process and resolve the remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-004-2 R3 (R3.1, R3.2) (MRO201100323)

During the MRO Compliance Audit, MRO determined that URE1 had a violation of CIP-004-2 R3 for failing to ensure that all employees with authorized cyber access to CCAs and unescorted physical access to CCAs had an identity verification. MRO discovered that one employee did not have a

complete Personnel Risk Assessment (PRA) in place for five months because the PRA did not include an identity verification.

A comprehensive review was conducted across the UREs. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

As a result of the internal review, the UREs identified a total of four individuals whose PRA dates fell outside the seven-year required period. For two individuals, access was removed and eventually restored. One individual had access removed and was notified of the screening requirement. One individual was a contractor who no longer required access.

Additionally, the UREs identified seven individuals who had not undergone an identity verification as required by CIP-004-2 R3.1. Two of the individuals did not have identification verifications because they had security freezes on their social security numbers. One of the seven individuals was a foreign national, and the UREs did not perform a passport verification. Additionally, three of the seven individuals had high levels of electronic and physical access rights to Critical Assets.

MRO determined that the UREs had a violation of CIP-004-2 R3 for failing to conduct PRAs with identity verifications and for failing to update each PRA at least every seven years.

MRO determined the duration of the violation to be from the earliest date a PRA was noncompliant through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the UREs perform multiple functions across multiple BPS facilities. Three of the individuals that did not have identity verification had high levels of access rights. One of the individuals was a foreign national for whom the UREs did not perform a passport verification.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

The UREs' Mitigation Plan required the UREs to:

1. update the master access list;
2. conduct a review of current PRA procedures to define further steps for conducting, reviewing, and reporting PRAs;
3. add an annual audit of the UREs' CIP master access list to the UREs' CIP procedures to ensure the PRAs are current and complete; and

4. review the PRA of each individual with CIP access to ensure they are current and complete, with seven-year criminal checks and identity verifications.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (MRO201100322)

During the MRO Compliance Audit, MRO determined that URE1 was in violation of CIP-004-1 R4. URE1 failed in three instances to update the list of its personnel who have authorized cyber or authorized unescorted physical access to CCAs within seven calendar days of any change. Specifically, two employees and one contractor had a change in job responsibilities, but URE1 did not update its list until over 20 days, over six months, and nearly one year later, respectively.

MRO determined that URE1 had a violation of CIP-004-1 R4 for failing to update its list of personnel who have access to CCAs within seven calendar days of any change.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 through when URE1 completed its Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Each of the three individuals continued to work at URE1. Each of the individuals retained the need for access, but that need was not documented. In addition, each of the individuals maintained up-to-date cybersecurity training and PRAs during the violation period.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. analyze, design, and implement an interim manual process to manage access control;
2. design a long-term, automated solution that automates the process of managing temporary or indefinite access needs upon employee/contractor status change (as identified from the human resources information system).
3. review and test the request form process workflow;
4. create a process to obtain a validation from the individual's manager for continued access upon any human resources information system change;

5. develop a new automated process to compare the human resources information system daily changes with the master access list. If an individual is found with a change and is on the master access list, the system will require validation to maintain access;
6. test enhancements;
7. communicate the new process to all managers; and
8. update related documentation to support the new process.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (R4.1, R4.2) (MRO2012010698)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-004-3 R4. URE2 and URE3 reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

Specifically, URE1, URE2, and URE3 (collectively, the UREs) failed to review quarterly the list of personnel with access to CCAs, update the list within seven calendar days of any change of personnel, and remove logical or unescorted physical access to CCAs within seven calendar days for personnel who no longer required such access.

The UREs identified less than one percent of individuals who did not have unescorted physical access to CCAs removed within seven days, as specified by CIP-004-3 R4. The unescorted physical access to CCAs was removed between 11 and 50 days from the change in status. The UREs' records indicate that none of the five individuals actually accessed any facility containing CCAs after their change in status.

The UREs also noted that URE3 failed to revoke physical access to URE3 CCAs for four individuals employed by a third-party entity that had access to URE3 substations. Access was removed for these four individuals between ten days and seven months after the change in status. None of the status changes were terminations for cause. A representative from the entity disclosed to URE3 that it had not always taken the proper steps to notify URE3 of the individuals' change in status. Without that notice, URE3 was unable to revoke access for terminations and transfers on a timely basis.

Additionally, the UREs noted that there was a lack of reliable connectivity between the UREs' physical access control system and card readers at particular URE3 and URE1 substations containing CCAs. As a result, six individuals (two for URE1 and four for URE3) were able to continue accessing those substations after their physical access was revoked in the physical access control system for periods

ranging from twelve days to six months. Because the individuals' access was removed in the physical access control system, they were not on the master access list, and their access was not reviewed on a quarterly basis.

Lastly, the UREs identified one instance where an employee transferred to a new job within the company and needed to retain access rights for a period of about two months after the transfer. The UREs failed to respond to an automated email alerting individuals of a need of change in access.

MRO determined that the UREs had a violation of CIP-004-3 R4 for failing to review quarterly the list of personnel with access to CCAs, update the list within seven calendar days of any change of personnel, and remove logical or unescorted physical access to CCAs within seven calendar days for personnel who no longer required such access.

MRO determined the duration of the violation to be from when the first individual's access was removed in the physical access control system but the individual still retained access at the card readers through when the UREs executed an agreement with the third-party entity mentioned above to monitor access to the UREs' CCAs.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The instances of access were for short durations involving individuals who had PRAs and had received the required cybersecurity training. In the instance where the transferred employee's access was not timely revoked, the employee's PRA and cybersecurity training were current. The inadequate process was limited to employee transfers. Other staffing changes such as terminations included all of the required information within the notification. Additionally, the communication issue between the physical access control system and card readers was limited to substations with low bandwidth communication.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. enhance the personnel change request form, which serves as official notification of a change in employee status, to include an area to identify whether the employee is a CIP employee. This change will allow for prioritization these forms;
2. develop and implement a disciplinary process to enhance management awareness of the importance of these forms;

3. implement a configuration update to the forms to hard code notifications to the appropriate departments, regardless of whether an invalid email address is manually entered on the form;
4. hold a meeting with the employees who are assigned to manage access to CIP-restricted areas to determine if there may be access control process and procedure efficiencies at the substations at issue;
5. hold a discussion with the third-party entity representative who manages CIP access controls to discuss the entity's commitment to implementing changes to prevent similar violations from occurring in the future;
6. implement a more formal agreement with the third-party entity, which will transition coordination with the entity and access control processes to the individuals who have more direct oversight of all individuals with authorized unescorted access to the CIP restricted area(s) within their respective locations;
7. review each site, individually and as a whole, to identify the root cause of the intermittent connectivity issue with the physical access control system and card readers. Staff tested solutions and implemented them at the affected sites; and
8. develop a monitoring and reporting tool to notify the UREs' security staff, which monitors the physical access control system, of any sites that have not connected. This report is sent every six hours.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R1 (R1.5) (MRO201100287)

URE1 submitted a Self-Report to MRO stating it was in violation of CIP-005-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-005-1 R1.5 to Cyber Assets used in the access control and monitoring of the ESP. These Cyber Assets consisted of a class of servers used to monitor, alarm, and log access to CIP substation ESPs. This system is used to access multiple Critical Assets and multiple CCAs.

The UREs failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, as required by CIP-007-1 R6. Due to incorrectly configured disk space overwrite settings, the UREs failed to perform a review of security event logs. When this

issue was discovered, the UREs took a snapshot of the active log data. From the snapshot log, the UREs found that the logs were incomplete and did not provide continuous security event data over the relevant time period. An in-depth analysis of the log generation and review process also identified a secondary automated script failure issue related to a previous upgrade in the scripting tool.

During mitigation, the UREs determined that there were additional issues with the servers as well as dial-up devices used to authenticate calls to the substation. The UREs failed to review or address certain alarm logs generated by both systems. The UREs failed to develop and implement testing procedures for evaluating adverse impacts of the security controls for the servers, as required by CIP-007-1 R1.

The UREs also failed to change shared passwords annually for the servers, as required by CIP-007-1 R5.3.3.

For URE1 and URE2, the UREs failed to perform a Cyber Vulnerability Assessment (CVA) for one year on these systems, as required by CIP-007-1 R8. Furthermore, in another year's CVA, the UREs failed to verify a list of ports and services required for operation were enabled, as required by CIP-007-1 R8.2.

MRO determined that the UREs had a violation of CIP-005-1 R1 for failing to afford several of the protective measures specified in R1.5 to Cyber Assets used in the access control and monitoring of the ESPs.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The UREs did not conduct an effective CVA in one year, and they did not remediate issues identified in the next year's CVA. As referenced in the CIP-003-1 R6 (MRO201100289) violation, the UREs did not implement CIP documentation change control during installation of the devices. During a CVA, the UREs discovered that they failed to maintain a list of certain ports and services, and they failed to remediate this issue by the following year's CVA. However, the risk posed by this violation was mitigated by several factors. Specifically, the UREs maintained a test environment and test procedures which specified a back-out plan for each change. While the UREs did not specifically test for adverse impacts on security controls, all changes had readily available plans to reverse any change that degraded security controls. Further, access to the affected system was only available through the UREs' corporate network, which then provided access to substations through a dedicated modem.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it was complete.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change two EMS shared account passwords;
3. design, develop, and test a manual log review process, review portions of the security event logs using the new manual process, and train the relevant team on the new manual log review process;
4. assess security monitoring processes for the devices to specifically address recipients of current automated alerts, action (response) plans for each recipient, and any other associated automated alerts;
5. change physical access control system and monitoring/logging server passwords for shared accounts where doing so did not pose unacceptable adverse impacts;
6. complete the investigation and verification for shared password accounts in the CIP environment;
7. complete the review and updating of policies, processes, and procedures to reflect accurate and up-to-date controls that address CIP-007 R5;
8. update process and procedure documentation to reflect responsibilities, actions performed, documentation created, and notifications made as part of the log review process;
9. investigate the ability to perform automated detection and alerting for issues affecting the log backup process;
10. draft action (response) plan for security events/alerts for affected devices, defining security event (rules with thresholds), response/action plan roles and responsibilities, and response action(s), among other items;
11. identify cybersecurity controls to be verified when a significant change is made. Controls to be verified include items such as audit log settings, password requirements, running services/open ports, default accounts, and so on;
12. communicate and train administrators on any changes to the processes and procedures to comply with CIP-007 R5;
13. complete the CVA action plan's last remaining item related to the affected devices, which was to investigate the ability to restrict access to a port on a modem;

14. finalize security event response (action) plans, update current processes and procedures, and draft communications to impacted teams;
15. consider and evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
16. test approved changes made to alerting processes;
17. develop process and procedure to compare established security controls before and after a significant change has been applied;
18. verify that all affected devices were identified and included within the scope of a subsequent year's CVA;
19. implement all approved changes and communicate to the appropriate resources;
20. select and retain consultant to perform and complete CVA of affected systems;
21. communicate and train administrative personnel on the process and procedure regarding determinations of whether cybersecurity controls are negatively affected by a significant change;
22. implement pilot test of long-term solution;
23. communicate and train administrators on the new tool, process, and procedure for shared password accounts;
24. implement test procedures to include verification that security controls in the monitoring/logging systems are not adversely affected by a change; and
25. implement long-term solution to improve management of shared password accounts within CIP environment and resolve remaining non-compliant shared account.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R1 (R1.5, R1.6) (MRO2012009900)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-005-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

Specifically, URE1, URE2, and URE3 (collectively, the UREs) failed to ensure that Cyber Assets used in the access control and/or monitoring of the ESPs were afforded the protective measures as specified in Standard CIP-007-1 R3 (patch management) and CIP-007-1 R5 (account management).

While gathering evidence to demonstrate that applicable security patches had been tracked, evaluated, tested, and installed for all Cyber Assets within the ESPs, the UREs discovered that non-Microsoft security patches were not included in the discovery and assessment phase of security patch management for some servers. The UREs had a patch management program in place to ensure applicable security patches are installed on these systems; however, non-Microsoft applications were not included within the scope of that program. The UREs did not properly assess patches for nearly 60 percent of the devices (the remaining applications had no patches over the period). Of those applications, the UREs' assessment deemed none of the patches applicable to the UREs' configuration.

Additionally, the UREs identified that a number of shared system accounts associated with the affected systems did not have all the necessary access controls in place as required by CIP-007-1 R5.1.3, CIP-007-1 R5.2.3, and CIP-007-1 R5.3 (see MRO201000232 and MRO2012009992).

The UREs reported the following: 1) shared system accounts, along with the name and title of the personnel who authorize access, were not maintained on a designated approvers list prior to a certain date; 2) documented access control procedures did not exist for managing access to these shared systems accounts and no annual reviews of the documented access controls had been performed; and 3) evidence of annual user access reviews did not exist. Further, some shared account owners did not identify a list of authorized users or maintain a usage log (audit trail) for their accounts. Additionally, some database shared account passwords were not changed annually. Mitigation was required for multiple user accounts, with two-thirds of those resulting in the account being deemed unnecessary and consequently removed.

In addition, the UREs later reported that they had discovered numerous changes that were made at Critical Asset substations. Simultaneous with reporting this information related to the instant violation, the UREs also submitted a Self-Report indicating that it was in violation of CIP-003-1 R6 (see MRO201100289). The UREs installed and modified Critical Asset substation ESP access points without subjecting them to a change control and configuration management process, resulting in these systems

not being tested for security controls prior to installation. Specifically, one substation ESP access point was replaced at a Critical Asset substation, and three new ESP access points were installed at new Critical Asset locations. None of the four changes was done in accordance with the UREs' change control and configuration management program. Because the change control and configuration management program was not followed, there was no documentation related to these ESP access points and no security controls testing was conducted prior to commissioning.

MRO determined that the UREs had a violation of CIP-005-1 R1 for failing to ensure that systems used in the access control and monitoring of the ESPs were afforded each of the protective measures specified in R1.5.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, there were a high number of accounts with incorrect access privileges. The UREs were unaware of which individuals had access and had not reviewed access or maintained logs. The UREs did not have adequate patch management procedures for the substation electronic access points, and they had incorrect documentation of the software baseline of the substation ESP devices. The UREs was not properly testing substation electronic access points for security controls when changes were made. There were several hundred CCAs that could be accessed using the electronic access points. Individuals would have had the ability to control BPS elements accessible through these points.

However, the risk was mitigated by the following factors. The only method to access the electronic access points at issue was from the UREs' network, which required authentication.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. complete an inventory of all applications that reside on the affected monitoring/logging servers to determine which applications are necessary and which can be removed;
2. assign responsibilities for the remaining applications to various URE groups to ensure that new security patches are discovered, assessed, and documented;
3. remove any unnecessary applications from the servers, following the UREs' change control process, and apply applicable security patches to necessary applications;

4. develop a procedure to discover, assess, and document new security patches regularly;
5. conduct a gap assessment to identify all shared, generic, or administrative accounts with access to the monitoring/logging application and servers;
6. develop training materials and train all affected account owners on the access controls and remediation required to bring all accounts into compliance with CIP-007 R5 requirements and subsequent CIP access control program;
7. have each account owner document his or her respective access control process and procedures for his or her respective account(s);
8. have each account owner review the user access privileges for his or her respective account(s) to confirm that they are correct and that they correspond with the appropriate business need to know;
9. assess, identify, and implement a solution for annual password changes for the database service accounts and update procedures and program documentation;
10. add the accounts to the designated approver personnel list along with the account owner's name and title; and
11. regarding test procedures, complete and document mitigating activities as part of the Mitigation Plan for MRO0201100289.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-005-1 R5 (R5.1, R5.2) (MRO201100288)

URE1 submitted a Self-Report stating that it was in violation of CIP-005-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

Specifically, during an internal inventory of substation Cyber Assets, URE1 and URE3 (collectively, the UREs) identified discrepancies between listed Cyber Assets and those deployed in the field. After further review, the UREs determined that certain substation ESP access points commissioned or decommissioned after a certain date had not been handled in a manner consistent with the UREs'

substation change control and configuration management process. As a result, the UREs failed to update documentation within 90 days of the change in two instances.

MRO determined that the UREs had a violation of CIP-005-1 R5 for failing to review, update, and maintain all documentation to support compliance with the requirements of CIP-005.

MRO determined the duration of the violation to be from the date when the UREs failed to update their documentation within 90 days as required by CIP-005-1 R5.2 through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This issue was limited to two 115 kV BPS facilities. In both cases, the devices that were installed were dial-up appliances that allowed remote access to CCAs with no routable connectivity outside the facility. The devices were accessible only from the UREs' corporate network through a special server used to communicate with the dial-up devices. Therefore, it was not likely that the installation of these devices would have an adverse impact on the security of the CCAs.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the UREs' pre-commissioning checklist;
3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;

9. inform MRO of status of contacting other utilities; and
10. execute the additional action plan to augment the substation change control process and resolve the remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.2, R1.3, R1.7) (MRO201100325)

During the MRO Compliance Audit, MRO determined that URE1 was in violation of CIP-006-1 R1. Specifically, URE1 failed to ensure and document that all Cyber Assets within an ESP also resided within an identified Physical Security Perimeter (PSP). MRO discovered several PSPs which failed to incorporate a completely enclosed six-wall border.

In one facility, MRO identified an opening in the six-wall border above the double doors leading from the main hallway into the PSP.

At another facility, MRO identified a non-continuous six-wall border a mechanical room.

MRO also determined that the physical security plan did not accurately reflect the current PSP configuration. URE1 relocated an access point and the access point's associated card reader. The changes undertaken as part of this project resulted in the redefinition of the PSP boundary. These changes were not listed in a version of the physical security plan over 30 days following the conclusion of the project. Therefore, MRO determined that the physical security plan was not updated within thirty days.

MRO determined that URE1 had a violation of CIP-006-1 R1 for failing to create and maintain a physical security plan that met all of the requirements of the standard.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 through when URE1 completed its Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PSP was within a secured building with security guards, surveillance cameras, and non-CIP card readers. The undocumented PSP configuration changes were properly documented approximately four months later. Both PSP openings were partially obstructed by conduit, wiring, and ductwork and were relatively small.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. improve CIP restricted area diagrams and replace existing diagrams with architectural drawings;
2. create a checklist that incorporates steps to update the physical security plan for each CIP restricted area;
3. complete an inspection of each CIP restricted area to identify, inspect, and ensure that a continuous six-wall perimeter is clearly defined and intact for each identified CIP restricted area;
4. provide a documented checklist that demonstrates that six-wall perimeters have been inspected;
5. create a document to be utilized each time a CIP restricted area has been identified as a construction project that may/may not change the PSP;
6. review the work order template and identify an area for a drop-down box that indicates work is adjacent or inside a CIP restricted area;
7. correct identified deficiencies in six-wall borders; and
8. submit work orders to the construction group to identify construction materials needed to ensure a continuous six-wall border for both PSPs and to complete the tasks as described in the work orders.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (MRO2012009899)

URE1 submitted a Self-Report to MRO stating it was in violation of CIP-006-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-006-1 R1 to Cyber Assets used in the access control and monitoring of the PSP.

The UREs failed to assess non-Microsoft patches (such as those for anti-malware software, backup software, and utilities) for their Cyber Assets that authorize and/or log access to their PSPs as required by CIP-007-1 R3. The UREs also failed to have all necessary access controls and procedures in place for

shared accounts on these same Cyber Assets, as required by CIP-007-1 R5.2. In addition, the UREs did not maintain evidence of annual user account access reviews, maintain a list of authorized users for shared accounts, enforce annual password changes, or maintain an audit trail for the shared accounts associated with these Cyber Assets, as required by CIP-007-1 R5.2.

Upon further review, the UREs discovered that they made numerous changes to PSP devices without following the CIP change control and configuration management process, as required by CIP-003-1 R6 (see also MRO201100289).

MRO determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protective measures specified in CIP-006-1 R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The UREs have multiple BPS facilities. The UREs had a high number of unnecessary accounts and accounts with incorrect access privileges. All of the shared accounts on these devices had compliance deficiencies: two-thirds of the accounts were removed, and the other one-third required some level of remediation. The UREs failed to review access or maintain adequate logs. The UREs had inadequate knowledge of the software baseline of their PSP devices or the procedures needed to patch these systems. The UREs did not have an inventory of installed software applications for devices used in the access control and monitoring of the PSPs. Of the "patchable" applications found on the UREs' PSP devices, the UREs failed to assess nearly 25% (although the UREs' assessment determined that none of the patches were applicable to their configuration).

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. document all installed applications on the physical access control system servers;
2. perform gap assessment for all accounts on the physical access control system application, database, and servers to identify business need for all generic, administrative, and shared accounts and determine gaps in access controls, and prepare report on findings;
3. assess and determine a solution for database service account annual password changes;

4. develop training plan for account owners, identify personnel, draft training materials, and schedule training dates;
5. develop a shared database password change remediation plan;
6. determine which applications are necessary to support critical functions and which applications could be removed from the servers;
7. determine which group is responsible for the discovery, assessment, and documentation of security patches for each application on the servers and assign ownership;
8. train relevant personnel on CIP-007 R5 access control requirements;
9. update the designated approver personnel list with the approvers and the associated accounts;
10. perform an access needs assessment for accounts;
11. establish a procedure to discover, assess, install, and document new security patches for assigned applications on a periodic basis;
12. assess, and if applicable, test, document, and install patches to bring applications up to date;
13. implement the database service account password changes;
14. submit appropriate requests to remove or modify accounts;
15. implement patch discovery, assessment, and implementation procedures on an on-going basis;
16. document CIP account access control procedures for the accounts in scope;
17. revise CIP access control program document to address or further clarify the requirements of CIP-007 R5; and
18. document the results of the account remediation plan, including, but not limited to, what accounts were remediated and what accounts were removed or disabled.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (MRO2012011501)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-006-1 R1. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which was consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures specified in CIP-006-1 R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

The UREs discovered that their physical security vendor made a change to their physical access control system without following the UREs' change control and configuration management process, as required by CIP-003-1 R6. The vendor also failed to ensure that significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls, as required by CIP-007-1 R1. The UREs did not perform any testing procedures as required by CIP-007-1 R1 when installing an update to two of the associated servers.

The UREs also discovered that a number of database user roles within their physical security system were mapped to security groups within the UREs' physical security system, but were not documented by the UREs, and the database user roles did not have passwords assigned to them as required by CIP-007-1 R5.2.

MRO determined that these issues were caused by a lack of communication with the UREs' physical security vendor and a lack of understanding by the UREs of their physical security system's configuration (which was installed by the vendor).

MRO determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protections specified in R1.8 to Cyber Assets used in the access control and monitoring of the PSP.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The UREs have multiple BPS systems, and the systems at issue had the ability to control physical access to all of the UREs' CCAs. The database user roles issue involved multiple, separate security groups and several active directory security groups associated with the UREs' physical security system. There were two accounts that had full access to the database for installation and configuration modification to all of the UREs' physical access control system. One of these accounts had inadvertent access for about a year. However, the risk posed by this violation was

mitigated by several factors. The vendor personnel who used the two accounts that had full access to the database had valid PRAs and cybersecurity training. Further, the risk associated with the update for a single change was minimal. Follow-up testing did not reveal any additional issues with the way the change was implemented, and the UREs did not identify any other instances of this issue.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. perform an access review on each identified security group and remove unnecessary access;
2. determine and implement security event monitoring and update associated documentation; and
3. update the designated approver personnel list and access control documents with information related to remaining security groups.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (SPP2012010242)

During the Joint Compliance Audit, SPP RE and WECC determined that URE2 and URE3 (collectively, the UREs) were in violation of CIP-006-1 R1. The UREs did not identify certain workstations used to provision access rights and to monitor alarms as physical access control system assets; therefore, the UREs could not provide evidence that the workstations were afforded all protective measures specified in CIP-006-1 R1.8.

The audit team found that unnecessary ports and services were enabled on certain URE3 physical access control system panel devices.

The audit team also found that antivirus signature files were not tested by the UREs before being implemented on the physical access control systems, as required by CIP-007 R4.2. The UREs asserted that they were relying upon the antivirus vendor to have tested the signature files before being published and that the risk of malware in the corporate network environment necessitated the immediate deployment of the anti-virus signature files upon receipt. This violation was determined to apply to URE1, URE2, and URE3.

SPP RE determined that the UREs had a violation of CIP-006-1 R1 for failing to afford several of the protective measures specified in R1.8 to Cyber Assets used the access control and monitoring of the PSPs.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs until mitigated.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not affording all protections according to CIP-006-1 R1.8 to the workstations, there was a risk that the physical access control system could have been compromised, leading to unauthorized access to CCAs. Having unnecessary ports and services enabled on the physical access control system panels devices presented the risk that a malicious actor might disable or render the panel devices inoperable. Because antivirus signature files were only tested in the vendor's environment, which is not representative of the UREs' environment, there was a risk that the UREs' ability to monitor and control their environment would have been affected upon installation of the signature files.

However, the risk was mitigated by the following factors. The workstations physically resided within a controlled-access area, and electronic access to the workstations was restricted to authorized users. The workstations were subject to the enterprise patch management program and were guarded by up-to-date anti-malware software. The UREs had disabled the unnecessary ports and services on the physical access control system panels following a CVA. Further, a failure of the physical access control system will not cause a loss of physical access control. Card readers will continue to authenticate access using the latest local database in the door control panels. Should the workstation used to provision access fail, access rights will not be able to be changed until the workstation is restored, but existing access rights will be preserved and used. A failure of the workstation used to monitor door alarms will result in loss of alarm monitoring ability on the affected workstation; however, there is redundancy, and the primary PSPs are manned at all times. No actual harm occurred to any of the UREs' Cyber Assets as a result of the violation.

The UREs' Mitigation Plan to address this violation was submitted to SPP RE.

The UREs' Mitigation Plan requires the UREs to:

1. replace the workstations with terminal server(s) and configure them for restricted access by appropriate personnel;
2. disable all unnecessary ports and services on the physical access control system panels that control CIP PSPs;

3. conduct a port scan to validate that all unnecessary ports were disabled;
4. establish a process to test the anti-malware signature files distributed by the UREs' anti-malware vendor;
5. review security/access controls to ensure the terminal servers comply with all applicable requirements of CIP-006-3 R2.2;
6. transition security operations center personnel from using local physical access control system clients to the terminal server client and ensure that all necessary functionality is available; and
7. remove the local installation of the physical access control system client from the local workstations.

CIP-006-3a R2 (R2.1, R2.2) (MRO201100290)

URE1 submitted a Self-Report stating it was in violation of CIP-006-3 R2. URE2 and URE3 also reported noncompliance to SPP RE and WECC, respectively, which were consolidated with the MRO violation for processing.

URE1, URE2, and URE3 (collectively, the UREs) failed to afford several of the protective measures in CIP-006-3a R2.2 to Cyber Assets that authorize and/or log access to the PSP.

The UREs failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, as required by CIP-007-3 R6. The UREs did not perform a review and analysis of Windows security event logs for the Cyber Assets that authorize and/or log access to the PSP. During a quarterly log review, the UREs discovered that the security event log was missing. The UREs' physical access control system servers were determined to have incorrectly configured disk space overwrite settings. An in-depth analysis of the UREs' log generation and review process also identified a secondary automated script failure issue related to a previous upgrade in the scripting tool.

After reviewing a snapshot of current logs, the UREs determined that the logs were incomplete due to a Windows log overwrite feature. The snapshot log did not provide continuous security event data over the relevant time period. During a preliminary review certain quarterly logs, the UREs also identified gaps in the Windows security logs.

During mitigation of the self-reported violations and the Joint Compliance Audit, the UREs determined that there were additional issues with the physical access control system. The UREs failed to develop and implement testing procedures for evaluating adverse impacts to the security controls for the

physical access control system. The UREs failed to change shared passwords for the system annually, as required by CIP-007 R5.3.3. Additionally, the UREs determined that a CVA was not performed for one calendar year on the system, as required by CIP-007 R8.

MRO determined that the UREs had a violation of CIP-006-3a R2 for failing to afford several of the protective measures in CIP-006-3a R2.2 to Cyber Assets that authorize and/or log access to the PSP.

MRO determined the duration of the violation to be from the first day of the quarter when the UREs were unable to review the previous quarter's security event logs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The physical access control system was used to monitor and control access to all of the UREs' PSPs. When the UREs performed a CVA, it discovered a "high risk" action item for the system's administrator accounts. Further, the UREs did not have a baseline list of approved ports and services for Cyber Assets used in the access control and monitoring of PSPs. Therefore, MRO determined that the failure to develop or implement test procedures, change shared account passwords, and conduct a CVA presented a serious or substantial risk to the reliability of the BPS.

The UREs' Mitigation Plan to address this violation was submitted to MRO stating it was completed.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change two EMS shared account passwords;
3. design, develop, and test manual log review process, review portions of quarterly security event logs using the new manual process, and train the relevant team on the process;
4. identify cybersecurity controls to be verified any time a significant change is made;
5. update process and procedure documentation to reflect responsibilities, actions performed, documentation created, and notifications made as part of the log review process;
6. investigate the ability to perform automated detection and alerting for issues affecting the log backup process;
7. correct all shared accounts discovered to be non-compliant where doing so does not pose unacceptable adverse impacts;

8. complete the investigation and verification for shared password accounts in the CIP environment;
9. complete the review and updating of policies, processes, and procedures to reflect accurate and up-to-date controls that comply with CIP-007 R5;
10. communicate and train administrators on changes to the processes and procedures to comply with CIP-007 R5 standard;
11. address three action items from the CVA, including correcting documentation to reflect a server determined to be needed for operation, removing a documented server no longer needed, and compiling list of approved services;
12. consider and evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
13. create process and procedure to compare established security controls before and after a significant change has been applied;
14. create a non-production test environment for the physical access control system application so that all desired changes can be tested for functionality and impact to cybersecurity controls prior to implementing change into the production environment;
15. communicate and train administrative personnel on the process and procedure;
16. communicate and train administrators on the new tool, process, and procedure for shared password accounts to ensure compliance with CIP-007;
17. implement test procedures to include verification that security controls in the physical access control systems are not adversely impacted by a change; and
18. implement long-term solution to improve management of shared password accounts within CIP environment and resolve remaining shared account at issue.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-006-3c R4 (MRO2012010967)

URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R4. URE1 failed to implement operational controls to manage physical access at all access points to the PSP at all times.

URE1's security personnel responded to a door alarm. Upon investigating the alarm, URE1 discovered that the employee pulled the door open without utilizing his badge, which serves as a unique identifier. Investigating further, the employee was observed leaving the area and tampering with the door latch to keep the door from securing when he left. Less than a minute later, when the same employee returned, he was able to enter the area without logging his access. At the time of re-entry, the latch was also returned to normal so the door would secure behind him.

MRO determined that URE1 had a violation of CIP-006-3c R4 for failing to implement operational controls to manage physical access at all access points to the PSP at all times.

MRO determined the duration of the violation to be for a brief time on the date when URE1 failed to implement operational controls to manage physical access.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The door latch was disabled for a short period of time, and the individual was in close proximity to the door while outside of the PSP. Additionally, URE1's physical access monitoring mechanisms were functioning properly at the time of the incident; the issue was identified because opening the door without first swiping a key card triggered the "forced door" alarm. Further, the facility at issue was continuously manned, and the operators could see the door from their stations. Also, the employee that tampered with the door had authorized, unescorted access to CCAs, had a current PRA, performed the required cybersecurity training prior to the incident, and had a valid business justification to be in the area.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it was completed.

URE1's Mitigation Plan required URE1 to:

1. place signs at access points stating that everyone must run his or her ID badge on the card reader;
2. have site management emphasize proper access controls; and
3. have the employee's manager confer with the individual employee responsible for the violation.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-006-3c R6 (MRO2012010966)

URE1 submitted a Self-Report stating it was in violation of CIP-006-3c R6. URE1 failed to log sufficient information to uniquely identify individuals and the time of access at all times. URE1 reported that it identified five separate occasions on which employees entered a designated PSP and did not comply with URE1's access control procedures, resulting in URE1's failure to log their access.

The first of the five instances occurred when URE1's security personnel responded to a door alarm. Upon investigating the alarm, URE1 discovered that an employee pulled the door open without using his badge, which served as a unique identifier. Investigating further, the employee was observed leaving the area and tampering with the door latch to keep the door from securing when he left. Less than a minute later, when the same employee returned, he was able to enter the area without logging his access. At the time of re-entry, the latch was also returned to normal so the door would secure behind him.

URE1's security personnel completes weekly "tailgating" assessments to ensure accurate and complete access logs. An individual engages in "tailgating" when he or she follows another individual with authorized access into a controlled access area without passing his or her badge by the card reader; as a result, the second individual's access is not logged. To complete the assessments, employees review access history reports and verify via camera that there is only one individual entry per card read or that the manual access log is utilized.

On one day, security personnel was completing a tailgating assessment and discovered two instances of tailgating. On two separate occasions, an employee with access to the area followed another individual into a facility without running his/her badge on the access control reader.

On a subsequent date, security personnel was completing another tailgating assessment and discovered two instances of tailgating. On two separate occasions, employees who had access to the area followed another individual into the area without running his/her badge on the access control reader.

MRO determined that URE1 had a violation of CIP-006-3c R6 for failing to implement the technical and procedural mechanisms for logging physical entry at all access points to the PSPs.

MRO determined the duration of the violation to be from the date URE1 first failed to uniquely identify individuals and the time of access through the date of the last instance and when URE1 resumed logging sufficient information.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In all five instances, the employees had authorized, unescorted access to CCAs, had a current PRA and cybersecurity training, and had a valid business justification to be in the controlled access area. In the instance where an employee tampered with the door lock, the facility was continuously manned, and the operators could see the door from their stations. Additionally, URE1 discovered the noncompliance through its proactive review process, promptly reported the issue to MRO, and has increased its awareness efforts.

URE1's Mitigation Plan to address this violation was submitted to MRO stating it had been completed.

URE1's Mitigation Plan required URE1 to:

1. engage in discussions with the managers of the employees, including security services staff, regulatory/compliance staff, and human resources staff. Since these discussions, management reinforced proper access controls with their entire facility staff; and
2. contact the managers of the individuals by the URE1 department responsible for recommending the level of discipline, and complete the disciplinary processes with the individuals responsible for the violations.

URE1 certified that the above Mitigation Plan requirements were completed. MRO verified that URE1's Mitigation Plan was complete.

CIP-007-1 R3 (SPP2012010241)

During the Joint Compliance Audit, SPP RE discovered that URE2 was in violation of CIP-007-1 R3. URE2 did not establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within its ESP.

Subsequently, the UREs performed a review of all Cyber Assets within the facility ESPs across all operating regions to identify any Cyber Assets not being managed in accordance with CIP-007-1 R3. In total, URE2 failed to include six Cyber Assets within an ESP in a patch management program, and URE1 failed to include over 20 Cyber Assets within an ESP in a patch management program. As a result, URE2 and URE1 (collectively, the UREs) failed to assess for applicability three patches associated with

five URE2 Cyber Assets and nearly 40 patches associated with 10 URE1 Cyber Assets. Two of the patches associated with URE1 Cyber Assets addressed software vulnerabilities.

SPP RE determined that the UREs had a violation of CIP-007-1 R3 for failing to include a number of Cyber Assets within ESPs within their patch management programs.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Out-of-date security patches could have allowed for unauthorized electronic access to, and potential compromise of, Cyber Assets within the ESPs. Such potential compromise could have resulted in a loss of monitoring or control capabilities for the UREs' facilities. Upon discovering the missing patches, the UREs performed an assessment and installed those patches that were applicable and necessary. Further, two of the missed patches addressed security issues. However, all other patches were optional in nature, as they were enhancements or addressed bug-fixes. None of the affected Cyber Assets were CCAs, and all of the affected assets resided within PSPs. All of the affected Cyber Assets were logically protected behind ESP firewalls requiring network access and authentication for remote access. None of the affected assets showed degradation of function from the failure to install patches, and there were no instances of malware or ESP-network intrusion.

The UREs' Mitigation Plan to address this violation was submitted to SPP RE.

The UREs' Mitigation Plan required the UREs to:

1. assess the patches that were missed and apply those that were deemed necessary;
2. review CIP-007-3 R3 security patch management with EMS personnel to ensure they understand the importance of security patch management;
3. review the security patch management process for all EMS team-controlled Cyber Assets to ensure the proper steps are fully documented;
4. identify opportunities for improvement in processes and collection of evidence to meet requirements and apply improvements to the security patch management process;
5. review, train, and reinforce the new processes and evidence requirements with staff in order to meet CIP requirements;
6. perform regular security patch management improvement validation on a sampling of patches to determine that evaluations are being performed in a timely manner.

The UREs certified that the above Mitigation Plan requirements were completed. SPP RE verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R5 (R5.2.3) (MRO201000232)

URE1 submitted a Self-Report to MRO stating that it was in violation of CIP-007-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

URE1 and URE3 (collectively, the UREs) failed to implement a policy for managing the use of accounts that limits access to only those with authorization and secures the account in the event of personnel changes, as required by CIP-007-1 R5.2.3.

The UREs reported that they failed to change shared account passwords in accordance with their policy based on the risk identified with the shared account passwords. The UREs' EMS account management policy provided for a shared account password to be changed within seven days if an individual with access to that account was terminated (unless the termination is for cause), or had a change in assignment in which he or she no longer needed access to the shared account.

However, in two instances where employees with access to EMS shared accounts resigned or retired, the UREs did not change the shared account passwords within seven days. The shared accounts at issue were for the EMS platform. In the first instance, the EMS user account employee resigned but the password was not changed until nearly three weeks later. In the second instance, an EMS administrative account user retired and the password was not changed until six months later.

The UREs' personnel with system administrator responsibilities had access to all of the functions within the EMS through a shared administrative account. For some individuals, the shared EMS administrative account could be accessed remotely through the corporate network or directly from certain consoles.

Although the shared passwords were not changed in accordance with the company policy, the two individuals at issue had no means of remotely accessing their EMS accounts seven days after their last date of employment with the company. Although the individuals could have accessed the EMS accounts by being physically at the CCA itself, the physical access for these individuals was revoked on their respective last days.

The UREs reported that the failure to change shared passwords arose because of a gap between the requirements of their policy and the specific procedure to implement the policy.

MRO determined that the UREs had a violation of CIP-007-1 R5 for failing to implement their policy for minimizing and managing the scope and acceptable use of administrator, shared, and other generic account privileges.

MRO determined the duration of the violation to be from when the UREs first failed to change the shared account password within the required seven days through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Since the individuals had their remote access credentials revoked, their only method of accessing the EMS administrative account would have been to either be physically at the server (which resided within a PSP to which they no longer had access) or to compromise the credentials of another employee.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. revise the subject procedure to address modifications of shared EMS account access passwords in the event of a change of assignment;
2. change the shared account passwords;
3. complete investigation and verification for shared password accounts in the CIP environment;
4. complete corrective action for shared accounts discovered at issue;
5. review and update policies, processes, and procedures to reflect accurate and up-to-date controls that address CIP-007 R5;
6. communicate and train administrators on changes to the processes and procedures;
7. evaluate longer-term solutions to improve the management of shared password accounts within the CIP environment;
8. implement pilot test of long-term solution;
9. communicate and train administrators on the new tool, process, and procedure for shared password accounts to ensure compliance with CIP-007; and
10. implement long-term solution to improve management of shared password accounts within CIP environment.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R5 (R5.3.1, R5.3.2, R5.3.3) (MRO2012009992)

URE1 submitted a Self-Report stating it was in violation of CIP-007-1 R5. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing. URE1 and URE3 (collectively, the UREs) failed to ensure that CCA passwords were changed at least annually.

URE1's EMS has a number of communication front-end (CFE) assets that facilitate communication with the EMS. There are four domain accounts set up to serve all of these CFEs. Only designated personnel with system administrator responsibilities have access to these accounts. URE1 discovered that EMS personnel had not changed the passwords on the four CFE asset accounts annually, resulting in non-compliance with CIP 007-3 R5.3.3. Upon discovery, the CFE passwords were changed.

URE3 discovered that EMS personnel had not changed the passwords on the four URE3 EMS domain accounts annually. These domain accounts were set up to serve all of URE3's CFE assets. Upon discovery, these CFE passwords were also changed.

The UREs initiated a review to determine if there were other accounts in the URE1 and URE3 EMS environments that had not had passwords changed annually. For the URE1 EMS environment, it was determined that a number of local administrator accounts for the CFE assets had not had passwords changed since their acquisition, which was prior to the date of mandatory compliance. These passwords were changed as they were discovered. For the URE3 EMS environment, it was determined that a number of local administrator accounts for the CFE assets had not had passwords changed annually, as well as the passwords for two application personal computers. Most had not been changed since prior to the date of mandatory compliance. These passwords were also changed as they were discovered.

During the course of mitigation of this violation, the UREs identified the need to file a TFE for the technical infeasibility of changing passwords on some accounts in use on EMS database servers. Additionally, through the mitigation efforts, MRO discovered that the UREs were relying solely on procedural controls for password changes on some accounts, without implementing technical controls as required by CIP-007-1 R5.

Additionally, SPP RE and WECC discovered issues with passwords on devices at Critical Asset substations during the Joint Compliance Audit. Specifically, the passwords on substation relays within the ESP did not meet the complexity requirements of CIP-007-1 R5.3. However, the issues were

mitigated through the submission of several TFEs, because the substation relays could not support the required password complexity rules.

MRO determined that the UREs had a violation of CIP-007-1 R5 for failing to require and use passwords subject to the complexity and change requirements of the standard.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a serious or substantial risk to the reliability of the BPS. The local administrator account on each CFE was not changed for a lengthy period. The CFE devices were the "front line" of the EMS, serving as the first line of communication that the EMS had with remote BPS facilities. While the UREs did not employ routable communications between Critical Asset substations and the EMS, they did use routable communications between two of the CFEs and some of the non-BPS substation facilities. The domain accounts that were originally identified and that could be used to access any of the CFE devices had not been changed in over a year. Further, a number of personnel with knowledge of these passwords left the employment of the UREs during the violation period.

However, the UREs configured firewalls between these two CFEs and those non-BPS facilities that limited the network traffic allowed from the remote terminal units into the CFEs. In addition, the UREs verified that no network connection has ever been initiated from these non-BPS facilities into these CFEs. Lastly, TFEs were appropriate for the EMS database issue, as the vendor did not support password changes for those accounts.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. train EMS staff on the CIP-007-3 R5.3.3 requirement;
2. place recurring reminders on the electronic calendars of EMS staff for changing the passwords in future years;
3. create recurring tracking items in the UREs' regulatory compliance database to provide a further level of notice/reminder/review and to ensure the password change is not missed in the future;
4. change passwords on all CFE domain and local administrator accounts; and
5. submit TFEs as necessary.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

CIP-007-1 R7 (R7.1, R7.2) (MRO201100292)

URE1 submitted a Self-Report stating that it was in violation of CIP-007-1 R7. URE3 also reported noncompliance to WECC, which was consolidated with the MRO violation for processing.

During an internal inventory of Cyber Assets within the ESP, URE1 and URE3 (collectively, the UREs) identified discrepancies between listed Cyber Assets and those deployed in the field. After further review, it was determined that certain substation CCAs decommissioned after a certain date had not been handled in a manner consistent with the UREs' substation change control and configuration management process.

During mitigation activities, the UREs determined that there were five instances of disposal or redeployment of substation CCAs subject to CIP-007 R7 (three for URE1 and two for URE3). Activities conducted for these changes did not follow the requirements of the UREs' substation change control and configuration management process.

MRO determined that the UREs had a violation of CIP-007-1 R7 for failing to implement their methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESPs.

MRO determined the duration of the violation to be from the date the Standard became mandatory and enforceable on the UREs through when the UREs completed their Mitigation Plan.

MRO determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The five devices consisted of three relays and two local control units. These devices were accessible only via dialup and did not communicate via routable protocol within the substation. Therefore, the information to be retrieved from these devices after their removal would have included only such things as protection system settings and device configuration, which would have presented a minimal risk to cybersecurity.

The UREs' Mitigation Plan to address this violation was submitted to MRO.

The UREs' Mitigation Plan required the UREs to:

1. implement the current internal change control process for changes to substation CCAs that were identified as not having followed the process;
2. implement a change to the pre-commissioning checklist;

3. conduct a review of the current substation change control process and submit a revised process for management review;
4. develop and deliver training on the revised substation Cyber Asset change control process to all personnel that have the potential to initiate a change to Cyber Assets in substations;
5. obtain management approval of the revised process and implement it using the new forms and procedures;
6. conduct an on-site review of Cyber Asset inventories at all substations identified as Critical Assets;
7. perform an analysis of discrepancies found during the inventory review and identify the root causes that led to the discrepancies;
8. develop an additional action plan of activities needed to address each cause identified as a source of the inventory discrepancies;
9. inform MRO of status of contacting the other utilities; and
10. execute additional action plan to augment the substation change control process and resolve any remaining issues.

The UREs certified that the above Mitigation Plan requirements were completed. MRO verified that the UREs' Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, MRO has assessed a penalty of one hundred and fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, MRO considered the following factors:

1. MRO did not consider the UREs' compliance history as an aggravating factor in the penalty determination;
2. the UREs had an internal compliance program at the time of the violation which MRO considered a mitigating factor;
3. MRO awarded significant mitigating credit to the UREs for their commitment to the development, implementation, and continuous improvement of their corporate compliance program;

4. the UREs committed to retain an independent, third-party consultant to evaluate opportunities for enhanced CIP management controls, both under the current requirements and in preparation for the transition to CIP Version 5, at an estimated cost of $205,000;
5. the UREs self-reported several of the violations;
6. the UREs were cooperative throughout the compliance enforcement process;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. the violations of CIP-003-2 R5, CIP-004-2 R3, CIP-006-1 R1, CIP-006-3 R2, and CIP-007-1 R5 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
9. the remaining violations posed a minimal or moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

As noted above, MRO awarded significant mitigating credit to the UREs' commitment to continuous improvement in the area of CIP compliance. The UREs' efforts to improve their program include reorganizing teams to create groups to enhance security through CIP compliance, conducting regular reviews of CIP compliance issues, creating and working through various project plans to improve their CIP cybersecurity posture, adding personnel, and instituting a robust Risk-Based Assessment Methodology.

After consideration of the above factors, MRO determined that, in this instance, the penalty amount of one hundred and fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

BOTCC reviewed the Settlement Agreement and supporting documentation on November 11, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by MRO as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Daniel P. Skaar* President Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 P: 651-855-1731 dp.skaar@midwestreliability.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sara E. Patrick* Vice President of Regulatory Affairs and Enforcement Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 P: 651-855-1708 se.patrick@midwestreliability.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and
Senior Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entities
Midwest Reliability Organization

Attachments

November 25, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity,
FERC Docket No. NP15-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE agrees and stipulates to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
WECC2013012579	CIP-002-2	R3; R3.3	High/ Severe	URE	$150,000
WECC2013012308	CIP-005-3a	R1; R1.5	Medium/ Severe	URE	
WECC2013012582	CIP-007-3a	R7; R7.1	Lower/ Severe	URE	
WECC2013012583	CIP-007-3a	R8; R8.2	Medium/ Severe	URE	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-2 R3; R3.3 (WECC2013012579)

WECC conducted an on-site Compliance Audit of URE (Compliance Audit). The auditors found that URE did not include relays at sites on its Critical Asset list as Critical Cyber Assets (CCAs). The auditors identified these devices as critical because they were classified by URE's CCA identification methodology as essential to the operation of the Critical Asset.

WECC determined that URE had a violation of CIP-002-2 R3 for failing to develop a complete list of CCAs essential to the operation of 11 Critical Assets.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the dial-up accessible protective relaying devices that were not identified as CCAs are capable of tripping transmission lines if the dial-up access capability is compromised. URE's failure to identify these devices as CCAs limited the protections afforded to these devices and increased the opportunity for intentional and unintentional misuse to occur. However, URE did apply some compensating measures. The dial-up accessible system was protected by authentication servers and dial-up gateway devices. The authentication servers were designed to prevent unauthorized access, and WECC reviewed the logs to verify that the servers denied unauthorized access.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. disconnect the dial-up remote access to the relays at Critical Asset substations that have energy management systems (EMS);
2. disconnect the dial-up access for relays at one Critical Asset substation which did not possess the equipment to provide EMS fault data reporting capability;
3. configure and connect EMS fault data reporting on the remaining relays identified as in scope for this violation and disconnect dial-up remote access; and
4. update URE's documentation used to determine what computer systems are CCAs to account for the NERC guidance document that clarifies the scope for dial up accessible devices.[4]

URE certified the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

[4] On June 17, 2010, NERC issued a guidance document named *Identifying Critical Cyber Assets (v1.0): Serial Cyber Assets that are Accessible via Dial-Up.* The document clarified NERC and WECC's approach to CIP-002.

CIP-005-3a R1; R1.5 (WECC2013012308)

URE submitted a Self-Report to WECC citing noncompliance with CIP-005-3a R1. URE reported that it failed to afford one of the protective measures specified in CIP-005-3a R1.5 to Cyber Assets used in the access control and monitoring of the ESPs. URE failed to document the assessment of 47 security patches for 38 electronic access control and monitoring devices (EACMs) within 30 days of being released, as specified in CIP-007 R3. Specifically, URE reported that its firewall vendor made 43 security patches available from its website. URE's assessment exceeded the 30 days allowed by CIP-007-3 R3.1 and URE's procedure. Further investigation found that URE's other firewall vendor made four security patches available. URE failed to document the assessment of these patches within 30 days.

WECC determined that URE had a violation of CIP-005-3a R1 for failing to afford one of the protective measures specified in R1.5 to Cyber Assets used in the access control and monitoring of the ESPs.

WECC determined the duration of the violation to be from 31 days following the release of the first set of security patches for EACM devices, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented around-the-clock logging and monitoring of all user access, and network traffic through and to the access points is sent to a centralized system to alert and dispatch personnel as necessary based on the type and level of anomalous activity. This would allow security personnel to block unauthorized access to the access points, thereby preventing compromise of CCAs within the ESP. URE also implemented a host-based intrusion detection system and antivirus tools which reside on most Windows Cyber Assets within the ESPs. This system can detect and prevent any anomalous activity based on malicious code signatures and other security thresholds set to alert appropriate security personnel. Detection of security vulnerabilities being exploited within the ESP was highly likely based on these detective controls. Detection of this type of activity would allow security personnel to disable communication through the access points to CCAs within the ESP, which would disable control from an outside attacker.

Further, if any anomalous activity resulting from exploitation of security vulnerabilities was detected, URE would have likely corrected the condition because URE implemented good corrective controls. Specifically, URE implemented redundancy in the access points protecting the control center ESPs, which would allow the entity to immediately recover if one of the access points failed. Also, URE would know immediately if any failures or suspicious traffic was occurring based on the logging of the access points, which would invoke security incident procedures or recovery procedures based on the

severity of the incident. The security personnel are trained on security incident analysis and how to recover from failures and incidents affecting Cyber Assets.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update a reoccurring task to provide automated email reminders to the Cyber Asset administrator(s);
2. update a reoccurring task to provide automated email reminders to the respective supervisor or manager assigned responsibility for the completion of firewall security patching; and
3. include notification to a department external to the firewall team for additional awareness of approaching deadlines and obligations ensuring task is completed in a compliant manner.

URE certified on that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R7; R7.1 (WECC2013012582)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R7. The audit team reviewed the disposal, redeployment, and media erasure/sanitation logs of randomly selected groups of Cyber Assets for the audit period and discovered five Cyber Assets where URE did not erase data storage media prior to disposal. The devices consisted of one Physical Access Control System (PACS) device and four non-critical Cyber Assets. URE provided evidence showing that one of the five devices had not been disposed of yet. URE was unable to provide evidence that the media was erased prior to disposal of the other four devices.

WECC determined that URE had a violation of CIP-007-3a R7 for failing to destroy or erase data storage media on four Cyber Assets to prevent unauthorized retrieval of sensitive cybersecurity data.

WECC determined the duration of the violation to be from when the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls that included physical security mechanisms with guards, special locks, closed circuit television, and logical perimeters, along with internal cybersecurity controls such as firewalls.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. add an IT security and compliance review to its change management procedures;
2. update its current checklist for hardware disposal;
3. add a peer review to the disposal and redeployment procedures;
4. create an inventory checklist destruction bin;
5. add a close-out peer review to the change management procedures; and
6. provide peer reviewer training.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-3a R8; R8.2 (WECC2013012583)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R8. Based on a review of URE's Cyber Vulnerability Assessment (CVA) procedures document, it appeared that the annotated tasks to perform a CVA review of Cyber Assets were "freeform and optional." URE's procedures allowed a vulnerability assessor to perform a subjective review of enabled ports and services on a subset of identified Cyber Assets. It also gave a vulnerability assessor the option to perform a subjective review of hardening statement, which equates to a subject matter expert reviewing a hardening document for a Cyber Asset to determine if the hardened configuration supports the required open ports and services. The assessor is also given the option to review the access control lists of access control systems to assess whether traffic restrictions are too lenient. None of the optional procedures annotated within the CVA procedures document would result in a deliverable that would demonstrate proof of compliance.

WECC determined that URE did not conduct a CVA of ports and services for all Cyber Assets. The scope of the violation includes over CCAs, over 30 non-critical Cyber Assets, over 20 EACMs, and less than 10 PACS devices.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to perform CVAs that included a review to verify that only ports and services required for operation of all Cyber Assets within the ESP are enabled.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to perform a CVA of Cyber Assets to ensure that only those ports and services required for normal and emergency operations were enabled could have led to a port or service of an associated critical application or system being unknowingly compromised. Such compromise could be used for a debilitating effect on the entity's multiple BES facilities.

However, URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms with guards, special locks, closed circuit television, and logical perimeters, along with internal cybersecurity controls, including firewalls, vulnerability scanning tools, intrusion detection systems, and a security events management system. Unauthorized access or other malicious use of the potentially vulnerable ports would have been difficult because the devices resided within an ESP and were actively monitored with a high likelihood of being detected upon compromise.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. tune its vulnerability identification tool for use in the annual CVA process and then run the tool in the production environment;
2. create and validate ports and services baseline with Cyber Assets administrators; and
3. perform updates to the annual CIP CVA procedures to ensure they are more specific and also to include the use of the tool.

URE certified that the above Mitigation Plan requirements were completed.

WECC has not yet verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's violation history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE self-reported the violation of CIP-005-3a R1;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of CIP-005-3a R1; R1.5 and CIP-007-3a R7; R7.1 posed a minimal risk to the reliability of the BPS, and the violations of CIP-002-2 R3 (R3.3) and CIP-007-3a R8 (R8.2) posed a moderate risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 11, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

In reaching this determination, the NERC BOTCC also considered the factors considered by WECC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 582-3918 – facsimile jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Christopher Luras* Director of Compliance Risk Analysis and Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile

Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

November 25, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. The violations resolved by this Settlement Agreement concern URE's operations in ReliabilityFirst, Midwest Reliability Organization (MRO), and SERC Reliability Corporation (SERC), herein

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

referred to as the "Regions." Following extensive coordination and collaboration among the Regions, ReliabilityFirst entered into the agreement on behalf of itself, MRO, and SERC.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed monetary penalty of seventy-five thousand dollars ($75,000), and an additional financial sanction in the form of a required investment of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. The violations in this Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013012304	CIP-002-1	R3	High/High	$75,000
RFC2012010916	CIP-003-3	R2	Medium/Severe	
RFC2012010917	CIP-003-3	R3	Lower/Severe	
RFC2012010328	CIP-004-3	R2	Lower/Severe	
RFC2012010918	CIP-005-1	R1.5	Medium/Severe	
RFC2012011084	CIP-005-3a	R1.5	Medium/Severe	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2012011370	CIP-005-2	R1.5	Medium/Severe	$75,000
RFC2013012307	CIP-005-1	R2	Medium/Severe	
RFC2013012318	CIP-005-1	R4	Medium/Severe	
RFC2013012319	CIP-006-2	R1	Medium/Severe	
RFC2012011366	CIP-006-2	R2.2	Medium/Severe	
RFC2012011373	CIP-007-1	R1	Medium/Severe	
RFC2012011372	CIP-007-2a	R2	Medium/Severe	
RFC2012010919	CIP-007-2a	R5	Lower/Severe	
RFC2013012439	CIP-007-2a	R6	Lower/Severe	
RFC2012011371	CIP-007-2a	R8	Medium/Severe	
RFC2013012320	CIP-008-1	R1	Lower/Severe	
RFC2013012321	CIP-009-1	R1	Medium/Severe	
RFC2013012463	CIP-009-1	R5	Lower/Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

Background Information

This Settlement Agreement resolves 19 CIP violations discovered through a series of Self-Certifications, Self-Reports, and a multiregional Compliance Audit (Compliance Audit). ReliabilityFirst led the Compliance Audit on behalf of itself, MRO, and SERC.

CIP-002-1 R3 (RFC2013012304)[4]

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-002-1 R3. URE failed to document the review of two types of Cyber Assets to determine whether those assets were Critical Cyber Assets (CCAs). Specifically, URE failed to identify time and frequency devices and certain laptop computers as CCAs.

In addition, URE permitted remote access to certain laptop computers, which were not identified as CCAs. These laptop computers were essential to the operation of URE's Critical Assets.

ReliabilityFirst determined the duration of the violation to be from the date the standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's method of identifying CCAs relies on a top-down approach that first considers essential functions, identifies applications that support those functions, and then identifies Cyber Assets that support the applications. This method did not directly review Cyber Assets related to each CCA and could have resulted in a failure to identify CCAs. Further, the two assets at issue could have led to significant harm to the BPS.

Several factors mitigated the risk. With respect to the time and frequency devices, ReliabilityFirst determined that the likelihood of a bad actor accessing URE's data system and reaching the assets at issue was low due to the defense-in-depth security strategies URE employs, including the containment of these assets behind multiple layers of physical and electronic access controls, the application of URE's change management process to these assets, redundant configurations, and the application of account and access management controls such as strong, two-factor authentication.

With respect to the laptop computers, URE required employees to sign into and be physically present in URE's facilities to take any actions affecting the BPS. Therefore, the employees could not take BPS-related actions using the laptops at issue.

[4] ReliabilityFirst applied the version of the Reliability Standard in effect at the time each violation began.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its CCA identification process to ensure that all Cyber Assets related to each CCA are identified and reviewed; and
2. create a business process diagram that includes a quality control check. The diagram is designed to ensure that all CCAs are considered.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-003-3 R2 and R3 (RFC2012010916 and RFC2012010917)

URE submitted a Self-Report stating that it had issues with CIP-003-1 R2 and R3. URE failed to document the delegation of responsibilities by its senior manager to delegates. In four instances, a CIP cybersecurity manager signed extensions to cybersecurity exceptions without being formally designated as a delegate. In addition, on three instances, the cybersecurity exceptions were not reviewed annually by the senior manager.

ReliabilityFirst determined that URE had violations of CIP-003-1 R2 and R3 because the entity failed to document the delegation of responsibilities by its senior manager to delegates.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to document the delegation of responsibilities to delegates, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation was documentation-related. Only one of the exceptions to the cybersecurity policy at issue was CIP-related. URE's mitigation strategy included appointing additional delegates, one of whom is the manager of cybersecurity. The manager of cybersecurity was qualified to review and approve the extensions, and was later designated to perform the task, as part of URE's mitigation.

URE's Mitigation Plan to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. obtain reviews and approvals by the appropriate CIP senior manager and document the appointment of delegates, including the manager of cybersecurity; and

2. conduct training on cybersecurity exceptions for the cybersecurity managers, their delegates, and for URE's cybersecurity department.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-004-3 R2 (RFC2012010328)

URE submitted a Self-Report stating that it had an issue with CIP-004 R2. As part of URE's annual review of its cybersecurity training program, URE attempted to update its program to incorporate information regarding cybersecurity threats. However, the training that URE finalized and adopted for use inadvertently omitted the information required by CIP-004-1 R2.2 regarding: i) the proper use of CCAs (R2.2.1); ii) electronic access controls to CCAs (R.2.2.2); and iii) recovery plans for CCAs after a Cyber Security Incident (R.2.2.4). URE used these training materials to provide training on two newly-hired employees and six newly-hired contractors.

In addition, during mitigation, URE identified an issue resulting from the conversion and re-formatting processes necessary to convert the training materials into the format utilized to train new employees.

ReliabilityFirst determined that URE had a violation of CIP-004-3 R2 because it failed to provide training that addressed all elements of this standard.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to include all required information in its training materials, through when URE submitted revised evidence of mitigating activities to include the issue identified during its initial Mitigation Plan implementation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All affected personnel had a personnel risk assessment and were eventually trained as required by the standard. The deficient cybersecurity training provided relevant information regarding preventing and defending against cybersecurity incidents, which was reinforced through URE's quarterly cybersecurity tips. The duration of the issue was limited due to the execution of URE's internal controls program.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. administer training to the individuals at issue; and

2. convert the cybersecurity training to a controlled document and conduct training on controls applicable to training revisions.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R1.5; CIP-005-3a R1.5; and CIP-005-2 R1.5 (RFC2012010918, RFC2012011084, and RFC2012011370)

URE submitted Self-Reports stating that it was in violation of CIP-005-1 R1.5. During the Compliance Audit, ReliabilityFirst discovered an additional instance of noncompliance with CIP-005-1 R1.5. In the course of mitigation, while implementing its improvement program, URE discovered an additional violation of this standard.

URE failed to: i) timely change passwords on 21 access control and monitoring devices (ACMs), CCAs, and non-CCAs; ii) locate two sets of ACMs in a Physical Security Perimeter (PSP) and afford the required protections; iii) afford the protections of CIP-007-1 R1 (test procedures) and R8 (cyber vulnerability assessment) to 52 ACMs; iv) consider electronic ACMs to be access points and afford the protections required by the standard; and v) identify additional access points to eight CCA servers.

ReliabilityFirst determined the duration of the first violation that was self-reported to be from the date the standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined the duration of the second violation that was self-reported to be from the date the devices were first commissioned into a facility not properly identified as a PSP, through when URE completed its Mitigation Plan.

ReliabilityFirst determined the duration of the third violation that was self-reported to be from the earliest date the devices at issue were commissioned, through the date the last two miscategorized devices were properly categorized and became subject to system administrator review.

ReliabilityFirst determined the duration of the violation discovered at the Compliance Audit and during mitigation to be from the date the standard became mandatory and enforceable, through when URE completed its improvement program.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to protect electronic security perimeter (ESP) access points and maintain secure passwords increases the likelihood of a gap in

security defenses for the ESP. The lengthy duration of the violations increased URE's exposure to this risk.

However, URE mitigated the risk by employing a defense-in-depth strategy that includes: i) a network operations center that actively monitors and responds to a host of enterprise-wide system performance and availability events. As a result, URE is capable of identifying any potentially disruptive network events before they impact BPS systems; ii) affording the assets at issue several protections, such as application of rigorous change management practices, consistent up-to-date patching, antivirus and malware prevention software, account and access management practices, and user and system logging and monitoring; and iii) locating the assets within controlled access facilities, which include protection against unauthorized physical access with multiple layers of electronic and physical access controls, such as guards, account management and access controls (e.g., strong, two-factor authentication). In addition, less than three percent of URE's non-user accounts had passwords that were overdue for change.

URE's Mitigation Plan to address the first self-reported violation was submitted to ReliabilityFirst. URE's Mitigation Plan required URE to:

1. change the passwords for all affected accounts; and
2. modify its process for creating new non-user accounts to require that accounts are monitored by its automated passwords management tool.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

URE's Mitigation Plan to address the second self-reported violation was submitted to ReliabilityFirst. URE's Mitigation Plan required URE to:

1. create documented PSPs for the facility that held the access control and monitoring devices;
2. validate that all protections associated with PSPs were present in the facility;
3. update employees' information; and
4. review its asset commissioning process to identify opportunities for improvement.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete. [5]

URE's Mitigation Plan to address the violation discovered at the Compliance Audit was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its cyber vulnerability assessment (CVA) and production readiness testing processes by defining criteria for justifications of firewall and access control list rule permissions; and
2. improve its processes to ensure that it conducts CVAs of non-critical Cyber Assets in, and electronic access points to, URE's ESPs and its ACMs.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (RFC2013012307)

During the Compliance Audit, ReliabilityFirst discovered that URE violated CIP-005-1 R2. URE failed to demonstrate that it enables only ports and services required for operations. For example, for one device, URE failed to explain how various network objects were used, and failed to provide a business justification for open ports and services.

ReliabilityFirst determined that URE had a violation of CIP-005-1 R2 because URE failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to restrict access to protected networks leaves those networks open to attack, which may make protected systems vulnerable to unauthorized access. The duration of the violation increased URE's exposure to this risk.

[5] URE completed the mitigating activities associated with the third self-reported violation prior to submitting the Self-Report. URE established processes for cybersecurity testing associated with significant changes, and assigned the devices at issue to the correct domain. In addition, some of the devices were decommissioned or were no longer listed on URE's ESP workbook or active within the ESPs.

URE's defense-in-depth strategies, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to improve its processes associated with defining criteria for justifications of firewall and access control permissions.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (RFC2013012318)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-005-1 R4 because URE failed to perform a comprehensive annual review of active ports and services.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed ongoing reviews on ports and services throughout the year as it made changes to its system. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), minimized the likelihood that an unauthorized person could access URE's data systems.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes associated with conducting CVAs of non-critical Cyber Assets and electronic access points to URE's ESPs and ACM devices; and
2. conduct a comprehensive annual review of all ports and services.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-2 R1 (RFC2013012319)

During the Compliance Audit, ReliabilityFirst discovered that URE had a violation of CIP-006-1 R1 because URE failed to contain all ESP Cyber Assets within a PSP.

Specifically, several PSPs at different locations had openings within the boundaries of the PSP that exceeded 96 square inches. Therefore, the PSPs did not provide a continuous six-wall boundary. In addition, the cabling between two rooms in one facility was not protected within a six-wall boundary. During the course of mitigation, URE discovered two additional PSP openings.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The openings at issue were obscured from observation because they were located above a dropped ceiling or below a raised floor. An individual attempting to exploit these unsecured openings would have required a special tool to access the openings.

In addition, the facility was staffed 24 hours a day, reducing the likelihood of unauthorized physical access. Access to any of the gaps would have been impeded by fire stop mechanisms, ductwork, wiring conduit, cable trays, or the steel infrastructure of the building. The location of the openings was within a restricted area with controlled access, camera surveillance, and other physical monitoring in place. The cabling between the two rooms in the facility had adequate defense-in-depth mechanisms and compensatory protective measures in place. URE's intrusion detection system and real-time monitoring of the Cyber Assets within the ESP remained intact throughout the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. close all of the PSP openings;
2. revise the PSP plan to require confirmation that all the requirements for implementing a new PSP or commissioning a new building are addressed;
3. institute annual physical inspections to ensure there are no openings within the PSP;
4. submit a technical feasibility exception (TFE) request for the cabling between the two facilities, which ReliabilityFirst approved; and

5. install permanent mesh to close off the tunnel and permanently secure the hatches.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-2 R2.2 (RFC2012011366)

URE submitted a Self-Report stating it was in violation of CIP-006-2 R2.2. During mitigation, URE discovered and self-reported an additional instance of noncompliance.

URE failed to afford certain protective measures to the access points to the ESP. URE improperly categorized 75 Cyber Assets and failed to afford these devices the cybersecurity testing required by URE's procedures. Also, URE's physical access badge reader system controllers were not categorized as Cyber Assets that authorize and log access to a PSP.

ReliabilityFirst determined that URE had a violation of CIP-006-2 R2 because URE failed to afford access points to the ESP certain protective measures.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to conduct cybersecurity testing leaves Cyber Assets vulnerable to attacks. The duration of the violation increased URE's exposure to this risk. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), mitigated the risk. In addition, URE regularly monitored logs from the affected devices, and it did not experience any Cyber Security Incidents for the duration of the violation.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. move the devices at issue into the correct domain of its device-tracking system;
2. improve its processes associated with ensuring that all Cyber Assets within an ESP reside within an identified, complete PSP;
3. ensure that all assets that control and/or monitor access to physical security systems are afforded all protections required by CIP-006 R2.2.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (RFC2012011373)

URE submitted a Self-Report stating it was in violation of CIP-007 R1. During the Compliance Audit, ReliabilityFirst discovered a second instance of noncompliance with CIP-007 R1. During mitigation, URE discovered two additional instances of noncompliance.

URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls. URE miscategorized 75 Cyber Assets and failed to afford these devices the cybersecurity testing required by URE's procedures and policy. In addition, URE: i) performed testing in its production environment rather than in an environment that reflects the production environment; ii) failed to perform cybersecurity testing for significant changes on certain turret servers;[6] and iii) failed to implement certain security patches.

ReliabilityFirst determined that URE had a violation of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's practice of testing in the production environment raised the risk of adverse actions occurring in the production environment when system changes are implemented. The lengthy duration of the violation increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk. URE's change management process, which requires thorough functional testing of significant changes, also reduced the potential for unauthorized access.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. re-categorize many of the Cyber Assets or remove them from the ESP;

[6] URE's turret servers are vendor-managed appliances identified as CCAs that support phone operations.

2. improve its processes associated with cybersecurity testing; and
3. create internal controls for the generation and maintenance of its software lists.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-2a R2 (RFC2012011372)

URE submitted a Self-Report stating that it was in violation of CIP-007 R2. During the Compliance Audit, ReliabilityFirst discovered an additional noncompliance of this standard. Finally, during mitigation, URE discovered and self-reported a third instance of noncompliance.

URE failed to ensure that only ports and services required for normal and emergency operations were enabled. URE failed to: i) perform its processes and procedures for ports and services review on 75 Cyber Assets; ii) demonstrate that only ports and services required for normal and emergency operations were enabled for multiple systems; and iii) review weekly enterprise security manager scans.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R2 because URE failed to maintain its process to ensure that only those ports and services required for normal and emergency operations are enabled.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to protect Cyber Assets within the ESP through a ports and services baseline increases the likelihood of a security gap. The lengthy duration of the violation increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) mitigated the risk. URE's network configuration is such that traffic is limited based on specific protocols, which are required to be met to enter the network. The configuration prevents unsolicited traffic from passing into the networks segregated by ESPs, thereby reducing the risk to the BPS. Additional protections are provided by intrusion detection and prevention system devices that are programmed to detect for malicious traffic attempting to gain access to the ESP, regardless of whether the ports and services are enabled on the end-device. If the intrusion detection and prevention system detects malicious traffic, it prevents the malicious traffic from gaining access to

the network. URE consistently maintained up-to-date patching for all devices at issue, and the devices were protected by antivirus and malware prevention software.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. enhance its processes for ensuring the security of access to and through its electronic access points as well as the security of non-Critical Assets in URE's ESPs and ACMs; and
2. improve its processes to ensure that only those ports and services required for normal and emergency operations are enabled through URE's improvement program initiative for baseline configuration data and configuration management.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-2a R5 (RFC2012010919)

URE submitted a Self-Report stating that it was in violation of CIP-007 R5.3.3. URE discovered that 21 (3%) of the passwords for 706 non-user accounts for CCAs, ACM devices, and non-CCA Cyber Assets within the URE ESP were not changed annually.

During the Compliance Audit, ReliabilityFirst discovered that URE failed to create historical audit trails of individual user accounts access activity. Also, for an approved TFE, URE indicated that a mitigating process was in place to change account passwords every 180 days, but one device did not have the technical capabilities to enforce that process.

During mitigation, URE discovered and self-reported an additional instance of noncompliance. URE's information application is deemed to be a CCA. URE failed to review certain accounts associated with this application during its quarterly entitlement reviews. In addition, certain active directory groups used for access to PI were not accurately reflected in quarterly entitlement reviews.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the account password issue was a documentation issue. Although URE failed to retain logs of sufficient detail to create historical audit trails of individual

user accounts, URE did produce, retain, and review logs of system security events. The logs at issue were for less than 10 % of the devices for which URE was logging and reviewing log activity. URE's network operations center actively monitors and responds to a host of enterprise-wide security tools and controls, which allows URE to identify any potentially disruptive network events and actual cybersecurity incidents before they impact systems related to the BPS.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

For a description of mitigating activities, see the Mitigation Plan for RFC2012010918, RFC2012011084, and RFC2012011370 described above.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-2a R6 (RFC2013012439)

URE submitted a Self-Certification stating that it was in violation of CIP-007 R6.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R6 because URE failed to ensure that certain Cyber Assets within the ESP had automated tools or organizational process controls to monitor system events that are related to cybersecurity.

During mitigation, URE discovered that it had not filed TFEs for logging on certain vendor-managed devices. URE failed to review access logs for three turret servers, which are vendor-managed appliances initially identified as CCAs located in three facilities.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE conducted undocumented reviews of turret servers access logs at one of the facilities approximately monthly. URE also conducted undocumented reviews for alarming of the access logs for the turret servers in two facilities daily. In addition, the telephony controlled by the turret servers could have been replaced by other means of communication in the event of disruption. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), reduced the likelihood of an unauthorized actor accessing URE's data systems.

URE took the following mitigating actions:

1. review the turret servers' access logs for the previous 90 days and develop, document, and implement a process for the ongoing monthly review of turret server access logs, including documentation and retention of the review results;
2. initiate coordination with the turret servers' vendor to develop a formalized process for the performance of cybersecurity testing on the turret servers and to evaluate implementing an automated logging solution on the turret servers; and
3. replace the process and technology used for security status monitoring and logging.

ReliabilityFirst verified onsite that URE completed these mitigating actions.

CIP-007-2a R8 (RFC2012011371)

URE submitted a Self-Report stating that it was in violation of CIP-007 R8. During the Compliance Audit, ReliabilityFirst discovered an additional instance of noncompliance with this Standard.

URE failed to include the required elements in its CVA of 93 Cyber Assets within the ESP. URE failed to: i) have a CVA process that applies to all applicable devices within the scope of the requirement; ii) conduct annual review of the list of ports and services required for operation; iii) provide sufficient evidence of a review of the controls for default accounts; and iv) document results for all CVAs. Not all documented CVAs included action plans for remediation or execution status of the action plans.

ReliabilityFirst determined that URE had a violation of CIP-007-2a R8 because URE failed to include the required elements in its CVAs of Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the earliest commissioning date of the devices at issue, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the failure to define adequately and execute CVAs increases the likelihood of compromise to the assets subject to CVAs. The duration of the violation and the number of devices involved increased URE's exposure to the risk.

URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370), minimized the likelihood of an unauthorized actor assessing URE's data systems. URE observed no breaches or Cyber Security Incidents during the time period of this issue. With regard to ports and services, URE runs enterprise security scans on some systems on a weekly basis to ensure that the systems are operating in accordance with the baseline. With regard to controls, the enterprise

security scans are used to identify, among other things, configuration of default accounts although it does not review controls for default accounts.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures associated with CVAs to ensure that all applicable devices are subject to a CVA; and
2. document the results for all CVAs and develop action plans for remediation or execution status.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-008-1 R1 (RFC2013012320)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-008 R1. ReliabilityFirst determined that, although URE has a Cyber Security Incident handling procedure, it did not include documented procedures to characterize and classify events as reportable Cyber Security Incidents.

ReliabilityFirst determined that URE had a violation of CIP-008-1 R1 because URE failed to include documented procedures to characterize and classify events as reportable Cyber Security Incidents in its Cyber Security Incident response plan.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of specific procedures to handle reportable Cyber Security Incidents could result in a delayed response to a cyber attack. The lengthy duration of the violation increased URE's exposure to this risk.

URE mitigated the risk by having in place documented procedures addressing all other elements of CIP-008, and URE experienced no Cyber Security Incidents through the duration of the violation. URE's defense-in-depth strategies reduced the likelihood of a bad actor accessing URE's data systems.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. integrate an incident criteria decision tree into its Cyber Security Incident response plan; and
2. add criteria to characterize and classify events as reportable incidents.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (RFC2013012321)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-009-1 R1. URE failed to create a recovery plan for CCAs. URE's yearly operational exercise, which used replicated backup (or "hot site"), was insufficient for disaster recovery of CCAs.

ReliabilityFirst determined that URE had a violation of CIP-009-1 R1 because URE failed to create a recovery plan for CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the use of a "hot site" leaves open the possibility that damage to Cyber Assets would be replicated to the only backup files, eliminating the possibility of restoration. The lengthy duration of the violation increased URE's exposure to the risk.

URE mitigated the risk by having mechanisms in place to protect CCAs against system events. URE not only backed up and stored the information required to restore CCAs, but was able to successfully restore various types of failed assets and data. Although URE's method of backup was insufficient for recovery purposes, it was sufficient for business continuity. URE's network operations center actively monitors and responds to a host of enterprise-wide system performance and availability events, which allows URE to identify any potentially disruptive network events before they impact systems related to the BPS. URE Cyber Assets were protected by firewalls, application of rigorous change management practices, consistent, up-to-date patching, antivirus and malware prevention software, account and access management practices, and user and system activity logging and monitoring. The assets were located within controlled access facilities, which provided protection against unauthorized physical access with multiple layers of electronic and physical access controls. URE's defense-in-depth strategy, as described above (see violations RFC2012010918, RFC2012011084, and RFC2012011370) also mitigated the risk.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures for recovering CCAs, backing-up and restoring those assets; and
2. ensure backup media required for restoring of these assets are properly tested.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R5 (RFC2013012463)

During the Compliance Audit, ReliabilityFirst discovered a violation of CIP-009-1 R5. URE failed to test its backup media annually.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE afforded its Cyber Assets other protective measures to reduce the risk of failure and to minimize threats and vulnerabilities. Those protective measures included: locating the Cyber Assets behind access points, including firewalls; rigorous change management practices; implementing electronic and physical access controls to all Cyber Assets within the ESP and ESP access points; implementing antivirus software where technically feasible; and implementing user and system activity logging and monitoring of access points and Cyber Assets within the ESP. URE had backed up and stored the information required to successfully restore CCAs in the form of the tapes and, upon testing the network device backup media during typical and frequent restorations of activities, URE regularly confirmed that information was available. URE had implemented other mechanisms to maintain the information essential to recovery. Although URE's method of backup was insufficient for recovery purposes, it was sufficient for business continuity.

URE's Mitigation Plan to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. improve its processes and procedures for recovering CCAs and backing up and restoring those assets; and

2. ensure backup media required for restoring of these assets are properly tested.

URE certified that the above Mitigation Plan requirements were completed. ReliabilityFirst verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a monetary penalty of seventy-five thousand dollars ($75,000) for the referenced violations. Further, as an additional financial sanction, URE shall provide evidence to demonstrate expenditures of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements. In reaching this determination, the Regions considered the following factors:

1. During the Compliance Audit, the Regions determined that all violations, when considered as a whole, represented a significant risk to the reliability of the BPS because they were a result of URE's weak cybersecurity compliance posture.
2. URE has prior violations of CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007. ReliabilityFirst determined that the Compliance Audit was URE's first comprehensive CIP audit and many of the prior violations presented limited risk to the BPS. Therefore, the Regions did not consider URE's violation history as an aggravating factor in the penalty determination;
3. URE had an internal compliance program at the time of the violation, and the Regions considered certain elements of the program as a mitigating factor in the penalty determination;
4. URE undertook above-and-beyond compliance measures. URE began implementing its improvement program, which is a coordinated, broad effort to improve its cybersecurity stance and compliance with CIP standards.
5. URE agreed to perform reliability enhancements and outreach efforts.
6. The Regions negatively considered the duration of many of the violations. Because of the lengthy duration, URE allowed an elevated risk of exploitation of its Cyber Assets.
7. URE self-reported several of the violations;
8. URE was cooperative throughout the compliance enforcement process;
9. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
10. Eighteen of the violations posed a minimal or moderate risk to the reliability of the BPS. The violation of CIP-007-2a (RFC2012011371) posed a serious or substantial risk to the reliability of the BPS, as discussed above; and

11. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the monetary penalty amount of seventy-five thousand dollars ($75,000) and an additional financial sanction requiring expenditures of at least one hundred thousand dollars ($100,000) in support of additional reliability enhancements, is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on November 11, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by the Regions, as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed monetary penalty of seventy-five thousand dollars ($75,000) and an additional financial sanction requiring the expenditure of at least one hundred thousand dollars ($100,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty
REDACTED FROM THIS PUBLIC VERSION

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org Kristina Pacovsky* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0670 (216) 503-9207 facsimile kristina.pacovksy@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Reliability First Corporation, Midwest Reliability Organization, SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violation[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE stipulates to the fact in the Settlement Agreement and admits that those facts constitute a violation of NERC Reliability Standards, and has agreed to a zero dollar penalty ($0), in addition to other remedies and actions to mitigate the instant

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

violation and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violation in this Full Notice of Penalty is being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013013030	CIP-007-3a	R3	Lower/ Severe	$0

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-007-3a R3 (RFC2013013030)

URE first contacted ReliabilityFirst to self-report its noncompliance with CIP-007-3a R3. URE followed up and submitted a Self-Report to ReliabilityFirst stating it had a violation of CIP-007-3a R3.

ReliabilityFirst determined that URE had a violation of CIP-007-3a R3 because it failed to implement its security patch management program when a URE employee backdated documentation related to URE's tracking of security software patches. Specifically, a URE supervisor had been backdating energy management system (EMS) patch logs.

For a period of approximately five months, a line item for one software application was accidentally omitted from the workflow list. Because of this omission, URE personnel were not reviewing whether security-related patches had been released for the software application. Once URE identified this issue, personnel reinserted the line item into the workflow list. However, the supervisor then modified previous versions of the log to appear as though personnel had been reviewing the software application during the five-month period.

For a period of approximately ten months, the supervisor backdated over 20 non-installation forms. The supervisor changed dates showing when the assessment or documentation was completed, to appear as though work was performed in a timelier manner than it was actually done.

The supervisor inserted and backdated a line onto the patch logs for the EMS to show that a single patch assessment was completed for one particular software patch. Personnel had completed the assessment on time, but the supervisor did not document this on the log until three months after the assessment—two months after it should have been added.

ReliabilityFirst determined the duration of the violation to be from the earliest date on which URE improperly recorded its patch assessment, through when URE terminated the supervisor and completed its mitigating activities.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE completed all patch assessments timely, as no patches were issued during the five-month period when the employee was not evaluating the software patches. Regarding the altered information that URE identified in its documentation, URE neither submitted the information to ReliabilityFirst during the course of a Compliance Audit, nor was it relied upon for URE's Self-Certifications to ReliabilityFirst as proof of compliance with CIP-007 R3. URE did not share the incorrect documentation externally in the compliance arena, self-discovered the issue, and remediated the violation prior to any transfer of information to ReliabilityFirst.

In addition to the risk posed by the violation, ReliabilityFirst also considered the wider potential reliability impact of an employee falsifying documentation. The falsified documentation could have affected not only records of compliance but the entity could also have used them in daily operations. The risk of the employee actions was mitigated because information shared by URE during the voluntary ReliabilityFirst performance appraisal demonstrated the noncompliance at issue was an isolated concern, and was not indicative of a wider workforce management performance failure. URE had in place internal controls and a compliance culture that self-identified, self-reported, and promptly addressed the actions of the employee responsible for the falsification. Finally, URE terminated the employee promptly after identifying the issue.

URE's mitigation activities to address this violation were submitted to ReliabilityFirst stating they had been completed.

URE took the following actions to mitigate this violation:

1. implemented a patch assessment control mechanism. This new mechanism reduced the risk of missing a patch assessment and ensures data integrity, thereby making backdating more difficult;
2. terminated the supervisor's employment and immediately disabled his physical and electronic access to all assets; and
3. assessed its workforce management (including hiring, training, and promoting employees) through a ReliabilityFirst-led appraisal.

URE provided evidence of completion that it had completed the above mitigation activities.

ReliabilityFirst verified that URE's Mitigation Plan was completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst did not assess a monetary penalty for the referenced violation. In reaching this determination, ReliabilityFirst considered the following factors:

1. URE voluntarily underwent a ReliabilityFirst performance appraisal of its management practices and procedures. Information received during this appraisal demonstrated that the noncompliance at issue was an isolated concern, and not indicative of any performance failure in the context of workforce management.
2. ReliabilityFirst determined URE's compliance history should not serve as an aggravating factor in the penalty determination;
3. URE had an internal compliance program at the time of the violation;
4. URE showed a clear commitment to strengthening its internal controls and preventing recurrence of noncompliance;
5. URE was able to detect and correct this violation because of improvements in its workforce management and internal controls;
6. URE self-reported the violation;
7. URE was cooperative throughout the compliance enforcement process;
8. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so, except by the lone supervisor;

9. the violation posed a minimal risk to the reliability of the BPS but did not pose a serious or substantial risk, as discussed above; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, a monetary penalty would not be appropriate for this violation.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 18, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violation at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by ReliabilityFirst as listed above, as well as the following factors:

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the no monetary penalty is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org

Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Kristina Pacovsky* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0670 (216) 503-9207 facsimile kristina.pacovksy@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1 and Unidentified Registered Entity 2
FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 2 (URE2), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because SERC Reliability Corporation (SERC) and URE1 and URE2 (collectively, UREs) have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the UREs neither admit nor deny the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

violations, but have agreed to the assessed penalty of one hundred twenty thousand dollars ($120,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
SERC2013012483	CIP-002-1	R3	High/ Severe	URE1	$120,000
SERC2014013371	CIP-003-3	R6	Lower/ Severe		
SERC2013012237	CIP-004-3	R4	Lower/ High		
SERC2013011770	CIP-005-1	R1.1	Medium/ Severe		
SERC2013012498	CIP-005-1	R1.1	Medium/ Severe	URE2	
SERC2013012488	CIP-005-1	R1.5	Medium/ Severe	URE1	
SERC2013012496	CIP-005-1	R1.5	Medium/ Severe	URE2	
SERC2013011754	CIP-005-2	R1.5	Medium/ Severe	URE1	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
SERC2013012240	CIP-005-3a	R3	Medium/ Severe	URE1	$120,000
SERC2013011761	CIP-006-1	R1.1	Medium/ Severe		
SERC2013012242	CIP-006-1	R1.8	Medium/ Severe		
SERC2013012244	CIP-006-1	R1.8	Medium/ Severe	URE2	
SERC2013012490	CIP-006-1	R3	Medium/ Severe	URE1	
SERC2013012495	CIP-006-1	R3	Medium/ Severe	URE2	
SERC2013011763	CIP-006-3c	R5	Medium/ Severe	URE1	
SERC2013012486	CIP-007-1	R1	Medium/ Severe		
SERC2013012487	CIP-007-1	R2.2	Medium/ Severe		
SERC2013012532	CIP-007-1	R3	Lower/ Severe		
SERC2013012243	CIP-007-1	R6	Medium/ Severe		
SERC2013012489	CIP-007-1	R8.3	Medium/ Severe		
SERC2013012491	CIP-009-1	R1	Medium/ Severe		

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-1 R3 (SERC2013012483)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R3. URE1 failed to identify all Critical Cyber Assets (CCAs) essential to the operation of its Critical Assets.

After an internal review, URE1 found workstations in separate Electronic Security Perimeters (ESPs) that it had originally classified as Cyber Assets within the ESP under CIP-005-1 R1.4 that it should have considered as CCAs under CIP-002-1 R3. Although not considered essential to the operation of the Critical Asset under its original assessment, these workstations did provide control capabilities and, if misused, could affect the operation of URE1's energy management system (EMS) and the bulk power system (BPS). SERC determined that URE1 was in violation of CIP-002-1 R3 because it failed to identify all CCAs that were essential to the operation of the Critical Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 added the misidentified Cyber Assets to the CCA list.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify Cyber Assets as CCAs could have left those devices without the required CIP protections, increasing the risk that the devices could be compromised and misused for malicious purposes. URE1 identified the workstations at issue as non-critical Cyber Assets within the ESP and protected them in the same manner it protected the identified CCAs. Use of the workstations required a user to be physically present at the workstations, and remote access was disabled. The first set of facilities, where approximately 90% of the workstations were deployed, were staffed 24 hours per day, seven days per week with operators and support staff as well as on-site security personnel. Moreover, a second set of facilities, containing approximately 10% of the workstations, had real-time security monitoring that included physical and logical access alarms and security cameras. URE1 had an intrusion detection system within the ESP monitoring for any port scans or pings against the EMS network. URE1 utilized a separate intrusion detection and prevention system on its ESP access point firewalls, behind which the workstations at issue resided. The workstations were within established ESPs and Physical Security Perimeters (PSP).

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. update its CIP-002 R3 procedure to include the concept of "compromise" in the CCA identification methodology because it was an identified root cause;
2. provide training to individuals affected by the update to the CIP-002 R3 procedure;
3. review and update the Cyber Asset/CCA list based on the updated CIP-002 R3 procedure;
4. update CIP-003 R6 procedures to address asset classification prior to the asset being implemented into production; and
5. provide training to individuals affected by the update to the CIP-003 R6 procedure.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-003-3 R6 (SERC2014013371)

URE1 submitted a Self-Report stating that it was in violation of CIP-003-3 R6. URE1 failed to follow its documented change control and configuration management process when updating malware prevention software on CCAs.

In URE1's change control and configuration management program, URE1 specified that any proposed changes hardware and software on Cyber Assets within the ESP should be documented through an internal change control management ticket which includes testing, approvals, and documentation. SERC determined that URE1 was in violation of CIP-003-3 R6 because it failed to follow its internal change control management process and updated malware prevention software on CCA workstations without following its documented change control and configuration management program.

SERC determined the duration of the violation to be from the date when URE1 mistakenly upgraded the malware prevention software without following its documented change control and configuration management process, until URE1 completed its testing of the cybersecurity controls.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 failed to follow its change control and configuration management program that allowed the implementation of untested changes to malware prevention software on CCAs. URE1 could have degraded existing cybersecurity controls or rendered the CCAs inoperable, reducing or eliminating URE1's ability to be aware of local system conditions or control its portion of the BPS. However, URE1 detected the update to the malware prevention software the following day and began investigating the scope of the issue. In addition, the change that URE1 implemented went through cybersecurity and functionality testing prior to deployment on corporate systems with no negative or adverse impacts to functionality or operations. URE1 also conducted after-the-fact testing and found no problems. System operators monitored the EMS 24 hours a day, seven days a week, and would have immediately noticed and reported to support personnel any system degradation. The EMS had security status monitoring in place to alert system administrators in the event the any malicious software was detected. The workstations were also within ESPs and PSPs, and physical and electronic access was limited to individuals who had completed personnel risk assessments and cybersecurity training.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. execute after-the-fact change control process;
2. analyze potential change control and configuration management sources of failure within groups that provide delegated operational support; and
3. develop and implement an action plan based on the results from the potential change control and configuration management sources.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (SERC2013012237)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-004-3 R4.1.

URE1 failed to update the list of personnel with access to CCAs within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel. The violation involved two instances of failure. In both instances, the individuals had physical access only, and the revocation failures resulted from the failure of staff to follow the URE1 access revocation procedures after the individuals' retirement or resignation. SERC determined that URE1 was in violation of CIP-004-3 R4 (4.1 and 4.2) because it failed to update its list of personnel with access to CCAs within seven calendar days of any change of personnel with such access to CCAs, and it failed to revoke access to CCAs within seven calendar days for individuals who no longer required such access.

SERC determined the duration of the violation to be eight days after the first individual retired until URE1 updated the access list and revoked the first individual's access rights, and eight days after the second individual resigned until URE1 updated the access list and revoked the second individual's access rights.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to revoke access to CCAs could have allowed former employees to use their credentials to gain access to and sabotage CCAs. However, both employees would have to obtain a key through their former supervisors to gain entry through a perimeter barrier before they would have been able to use their physical access badge to access the PSP. Both employees were in good standing with URE1 prior to and after their departure. Neither employee used their cards to access any PSP or site after the date of their respective retirement and resignation. The revocation of access occurred six days and eleven days late, respectively.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. develop reinforcement training for individuals who have the ability to initiate off-boarding processes in the human resources system. The training would concentrate on the importance of timely data entry and possible compliance implications of late data entry;
2. develop training for managers who have direct reports with NERC CIP access. The training would concentrate on the importance and expectations of the manager's role in the off-boarding process;
3. implement reinforcement training in the learning management system; and
4. assign and schedule respective reinforcement training to be completed by any individuals identified.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-005-1 R1.1 (SERC2013011770)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-3a R1.1. URE1 failed to identify externally connected dial-up modems, terminating at devices within ESPs, as ESP access points.

URE1 had mistakenly identified the wrong devices as access points for some facilities' ESPs. Dial-up gateways secured, authorized, and managed remote access to the facilities, and once the security packets for the individuals accessing were authenticated at the gateways, modems permitted access to the CCA. Originally, URE1 had identified the gateways as access points. Instead, it should have identified the interior modems as the access points because the modems represented externally connected communications endpoints, terminating at any device within the ESP. URE1 should have identified the gateway devices as electronic access control and monitoring (EACM) devices, which performed the access control, authentication, monitoring, and reporting functions on behalf of the modems. In addition, URE1 failed to identify access points into the ESP for serially connected non-essential Cyber Assets that resided outside of the ESP.

URE1's failure to identify the access points stemmed from a flawed interpretation of a NERC compliance guidance document. URE1 had erroneously determined that Cyber Assets non-essential to

the operation of Critical Assets that were serially connected to Cyber Assets within the ESP did not have to be classified as access points or as being associated with access points.

SERC determined that URE1 was in violation of CIP-005-3a R1.1 because it failed to identify all ESP access points.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify and designate access points to the ESPs increased the risk of unauthorized access to the implicated ESPs.

Regarding the failure to identify modems as access points, URE1 placed the modems behind secured gateway devices that were providing both access control and authentication functions. As a result, all access attempts arriving at the modems would first have had to pass through the gateway, effectively ensuring that CCAs to which the modems connected were shielded from unauthorized access. Consequently, the failure to identify the modems as access points was an error in documentation.

Regarding the non-routable connections crossing into the ESP, URE1 protected the Cyber Assets that serially communicated with devices inside the ESP within secured facilities or resided inside locked cabinets or cages, and URE1 identified and documented the devices. Additionally, the non-routable nature of the communications technically limited the provision of perimeter protections where such serial communication links are utilized. During the violation, there were no known adverse or negative impacts from not identifying access points for serial (non-routable) connections.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. identify modems as access points for all dial-up accessible facilities;
2. disconnect the modems at several critical facilities;
3. deem one facility not critical through the execution of the risk-based assessment methodology (RBAM);
4. modify its Cyber Asset identification tool to add instructions which would ensure that modems associated with dial-up access are identified as access points;

5. modify its CIP-007 R1 test plan to ensure that modems associated with dial-up access are identified as access points;
6. provide training to the individuals affected by the changes;
7. update ESP diagrams to identify protocol converters as access points;
8. submit Technical Feasibility Exceptions as appropriate for the functions that could not be performed at the access points;
9. update the CIP-007 R1 test procedures to ensure that serial devices connected from outside the ESP have an access point to a device inside the ESP; and
10. provide training for the individuals affected by the procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was completed.

CIP-005-1 R1.1 (SERC2013012498)

SERC sent URE2 an initial notice of a Compliance Audit. Following the notice, URE2 submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.

URE2 failed to identify access points into the ESP for serially connected non-essential Cyber Assets that resided outside of the ESP. URE2 reported that Cyber Assets residing outside of the ESP were serially connected to devices within the ESP and documented, but no access point for the connection was identified.

Within the Critical Assets at issue, URE2 had serial (non-routable) connections from various non-essential Cyber Assets outside of the ESP that connected directly to human-machine interface machines or switches that were identified as CCAs and protected as such. URE2 also had serial connections from non-essential Cyber Assets outside the ESP to protocol convertors that were identified as non-critical Cyber Assets within the ESP and protected as such. The serial connections did not traverse any Cyber Asset boundary device on the ESP that would be considered an access point under CIP-005-1 R1.

URE2's failure to identify the access points stemmed from a flawed interpretation of a NERC compliance guidance document. URE2 had erroneously determined that Cyber Assets non-essential to the operation of Critical Assets that were serially connected to Cyber Assets within the ESP did not have to be classified as access points or as being associated with access points.

SERC determined that URE2 was in violation of CIP-005-1 R1.1 because it failed to identify all ESP access points.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 executed an out-of-cycle RBAM and determined it had no CCAs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify and designate access points to the ESPs increased the risk of unauthorized access to the involved ESPs. However, the Cyber Assets that serially communicated with devices inside the ESP were protected within secured facilities or resided inside locked cabinets or cages, and the devices were identified and documented by URE2. Additionally, the non-routable nature of the communications technically limited the provision of perimeter protections where such serial communication links are utilized. During the violation, there were no known adverse or negative impacts from not identifying access points for serial (non-routable) connections.

URE2's Mitigation Plan to address this violation was submitted to SERC.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE2 certified that the above Mitigation Plan requirements were completed. SERC verified that URE2's Mitigation Plan was complete.

CIP-005-1 R1.5 (SERC2013012488 and SERC2013012496)

SERC sent URE1 and URE2 an initial notice of a Compliance Audit. Following the notice, URE1 and URE2 each submitted a Self-Report to SERC stating that they were in violation of CIP-005-1 R1.5. URE1 and URE2 failed to properly identify certain EACMs and afford certain EACM devices the protective measures specified in CIP-009 R1.

During an internal review, URE1 and URE2 discovered that each had failed to identify network management devices as EACMs based on an incorrect interpretation of the Requirement, despite previously identifying and protecting them as EACMs. SERC determined that several authentication servers included in the Self-Reports were not EACMs and should not have been included.

Additionally, URE1 and URE2 discovered that each had failed to afford other EACMs the protective measures specified in CIP-009 R1. URE1 and URE2 failed to document the steps necessary for the recovery of firewalls within their existing CIP-009 R1 recovery plans.

SERC determined that URE1 and URE2 were in violation of CIP-005-1 R1.5 because each failed to identify properly certain EACM devices and failed to afford certain EACM devices the protective measures specified in CIP-009 R1.

SERC determined the duration of the URE1 violation to be from when the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined the duration of the URE2 violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 implemented an off-cycle RBAM and determined that it does not have any CCAs.

SERC determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify properly the management devices as EACMs posed a risk that URE1 and URE2 might not have applied appropriate controls to prevent the theft or modification of authentication credentials or prevent the alteration or disablement of access control rules. Additionally, the failure to include the firewall EACMs in the CIP-009 R1 recovery plan posed a risk that URE1's and URE2's ability to recover the firewall EACMs might be delayed unnecessarily, and thereby impact URE1's and URE2's overall ability to protect and remotely operate its Supervisory Control and Data Acquisition system.

However, regarding the management EACMs, access to the devices was restricted to CIP-authorized personnel and required two-factor authentication. The devices were protected within a secured PSP and resided behind a corporate firewall. No known instances of unauthorized physical or electronic access to the management EACMs occurred during the violation.

Regarding the firewall EACMs, although not part of the CIP-009 R1 recovery plan, recovery plans were available to the technicians that were responsible for the recovery of the firewalls. Moreover, operational recovery of the devices was required on at least two occasions. URE1 and URE2 provided evidence of the device recovery, which indicated they successfully recovered the devices with no undue delay.

URE1's and URE2's Mitigation Plans to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. complete an analysis of its policies, standards, and guidelines for EACMs to determine what controls should be included in distributed enterprise security CIP-003 through CIP-009 procedures;

2. update the relevant procedures, including relevant supporting documentation and references;
3. provide training for individuals affected by the procedural changes;
4. apply controls identified above and prepare evidence to demonstrate compliance with updated procedures; and
5. perform an exercise pursuant to CIP-009 R2 on the updated recovery plans.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE1 and URE2 certified that the above Mitigation Plans requirements were completed. SERC verified that URE1's and URE2's Mitigation Plans were complete.

CIP-005-2 R1.5 (SERC2013011754)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.5.

SERC later determined that the violation began when Version 2 of the CIP Standards became mandatory and enforceable. URE1 failed to ensure that Cyber Assets used in the EACMs of the ESP at its facility were afforded the protective measures specified in CIP-006-2 R3. After the initial discovery of its failure to protect EACMs within a fully enclosed PSP at one facility, URE1 identified additional EACMs residing within a PSP that lacked complete six-wall boundaries at a second facility.

During a review of the PSPs, URE1 discovered three openings greater than 96 square inches under the raised floor below the facility's PSP and nine openings greater than 96 square inches above the false ceiling in a second facility's PSP. The identified openings resulted from URE1's reliance on the erroneous statements of a third-party vendor that it had installed wire mesh in all openings exceeding 96 inches prior to the date of mandatory compliance.

SERC determined that URE1 was in violation of CIP-005-2 R1.5 because it did not afford EACM devices the protective measures specified in CIP-006-2 R3.

SERC determined the duration of the violation from the date the Standard became mandatory and enforceable on URE1 until URE1 closed the openings in the PSPs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to create complete six-wall boundaries protecting EACMs could have allowed

intruders to gain physical access to the EACMs and allowed them to manipulate or destroy the devices. The root cause of the identified violations stemmed from URE1's reliance on the assertions of a third-party consultant. However, the affected PSPs were within existing corporate computer rooms that were restricted to corporate Information Technology personnel. The facilities at issue had on-site physical security staff that monitored the premises 24 hours a day, seven days a week. The EACMs were monitored by an intrusion detection system, which would alert URE1 staff to any unauthorized attempts to interface with the EACMs.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. meet with responsible persons to discuss an appropriate design solution to block the openings;
2. conduct inspections at additional PSPs; URE1 determined that they were properly enclosed by a six-wall border;
3. work with responsible persons to improve the facilities change management process to ensure that the PSPs are appropriately secured from the compliance date forward and further, that changes are not made that compromise PSPs. Specifically, the revised process would ensure that area owners submit a request form to corporate security for approval when establishing a NERC CIP PSP or prior to initiating any changes. This form would trigger a review by corporate security to ensure that proposed plans are consistent with NERC CIP physical security requirements;
4. evaluate vendor proposals based on the design solution and completed work;
5. work with vendors to ensure that all gaps in wire mesh have been corrected with installation of additional wire mesh. Area owners worked with a vendor to seal the heating, ventilating, and air conditioning ducts; and
6. conduct inspections at the remaining PSPs to ensure they are properly enclosed by a six-wall border.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-005-3a R3 (SERC2013012240)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-3a R3.

URE1 failed to implement electronic processes for monitoring and logging access at an access point to the ESP 24 hours a day, seven days a week.

During an internal review, URE1 discovered a single ESP access point where it had not enabled access logging for approximately 8% of the configured security policies for that access point. A URE1 firewall analyst had implemented the policies, but failed to configure fully the logging command. The policies represented access permit statements, which were enabled to allow several host machines to communicate with a field data concentrator residing inside an ESP.

SERC determined that URE1 was in violation of CIP-005-3a R3 because it failed to implement electronic processes for monitoring and logging access at an access point to the ESP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from when URE1 implemented the new firewall policies on the facility firewall but failed to enable logging on the firewall policies, until URE1 implemented logging on the firewall policies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 failed to monitor or log access to an ESP access point that could have left it unable to identify unauthorized access across the ESP access point if the access involved the four policies. Such a situation could have left URE1 unable to analyze any such unauthorized access and respond to prevent similar incursions. However, the policies had been established in accordance with URE1's procedures, including the restriction of access to authorized personnel. All traffic from the host devices was encrypted via a virtual private network tunnel. The failure was limited to a single access point and affected approximately 8% of the security policies established for that access point.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. enable logging on the four policies;
2. update its CIP-005 procedure to institute an independent review process for firewall policy changes; and
3. provide training for individuals affected by the procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.1 (SERC2013011761)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.1. URE1 failed to establish a completely enclosed (six-wall) border for an identified PSP and had not deployed and documented alternative measures to control physical access.

During an internal review, URE1 discovered it did not have a fully enclosed six-wall border at two PSPs. The previously unidentified openings were above false ceilings and were greater than 96 square inches.

In addition, where URE1 could not establish a completely enclosed (six-wall) border around network wiring as required, in two instances URE1 did not deploy and document alternative measures to control physical access to wiring.

SERC determined that URE1 was in violation of CIP-006-1 R1.1 because it failed to establish a completely enclosed (six-wall) border for multiple identified PSPs and had not deployed and documented alternative measures to control physical access.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1's failure to identify openings in PSPs and provide alternative measures of protecting ESP wiring external to a PSP could have allowed an intruder to gain access to CCAs within the PSP or to intercept, manipulate, or degrade ESP communications on the unprotected ESP wiring.

Regarding the first PSP discovery, the unidentified opening was approximately 30 feet above the floor. An intruder would have required rappelling equipment to gain access to the facility and would have entered the room in full view of the operators and any other occupants. The facility was access-controlled and staffed 24 hours a day, seven days a week. The opening was only accessible from an area that had corporate access controls with restricted access.

Regarding the second PSP discovery, the unidentified openings were approximately 30 feet and 20 feet above the floor, respectively. The unsecured openings were within an access-controlled facility that had on-site security staff 24 hours a day, seven days a week. A potential intruder would have to discover the openings above a false ceiling before attempting to gain access to the PSP using those openings.

Regarding the ESP wiring discovery, the ESP wiring in both instances was located within a secured corporate facility that on-site security personnel monitored 24 hours a day, seven days a week. A potential intruder would have to discover the ESP wiring above a false ceiling or below a raised floor before attempting to access it for malicious purposes.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. work with its facilities group to block the openings;
2. work with responsible persons to improve the facilities change management process to ensure that PSPs are appropriately secured from the compliance date forward and that further changes are not made which compromise PSPs. Specifically, the revised process ensures that area owners submit a request form to corporate security for approval when establishing a NERC CIP PSP or prior to initiating any changes to a PSP. This form triggers a review by corporate security to ensure that proposed plans are consistent with NERC CIP physical security requirements;
3. conduct inspections at the remaining PSPs to ensure they were properly enclosed by a six-wall border;
4. re-designate a PSP to include areas where ESP wiring spanned outside the identified PSP;
5. pull armored fiber optic cable to replace the existing fiber wiring which spanned outside the identified PSP;
6. update corporate security processes to include an assessment of network wiring before the creation of a PSP or the re-designation of an existing PSP;
7. provide training for the individuals affected by the revised corporate security process referenced above;
8. review all PSPs to determine which ones require further action to ensure network wiring is being afforded the proper protection pursuant CIP-006 R1.1; and
9. address and bring into compliance any additional issues identified during the review.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (SERC2013012242)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8.

URE1 failed to afford Cyber Assets used in the Physical Access Control Systems for the PSPs the protective measures specified in CIP-007-1 R1, specifically the testing of cybersecurity controls prior to implementing significant changes.

Firstly, URE1 discovered 74 instances where it had not tested PACS cybersecurity controls prior to implementation of significant changes into production. In 22 instances, URE1's test plans only called for testing to ensure the devices still functioned as expected but did not call for testing for any changes to the existing cybersecurity controls. In 17 instances, URE1 failed to implement the cybersecurity controls portion of the existing test plan. In 28 instances, URE1 failed to test any cybersecurity controls on several failover PACS servers because personnel failed to recognize the servers were PACS devices. Finally, there were seven instances where URE1 failed to document that any required testing had been conducted.

Secondly, URE1 failed to afford PACS devices the protective measures specified in CIP-007-1 R3 by failing to assess a security patch for certain PACS components within 30 days of release. URE1 identified a missed assessment of a database security patch. This was the only missed PACS database server patch, and it only applied to two PACS database servers, consisting of a primary server and a standby server.

Thirdly, URE1 discovered a single shared account with read-only access to the PACS was not afforded the protective measures specified in CIP-007-1 R5. This specific account was established on the PACS database server prior to the date of mandatory compliance so that individuals could run nightly reports that were used to manage and review access rights to the URE1 PSPs. Although this shared account was included in quarterly reviews, it was not afforded the protective measures required for shared accounts due to confusion between two teams regarding who was responsible for management of the account.

Finally, URE1 also implemented a change to its PACS production servers without following its documented change management procedures required by CIP-003-3 R6.

The URE1 procedure for change management required all significant changes for PACS to be held out of regular implementation pending a more extensive documented review and testing sessions. In the event that testing in the URE1 quality assurance environment produced negative results,

implementation into production would be halted until resolved. URE1 supplemented the process that described how its personnel would use the change management system to document any requested change to the PACS. URE1 process required the change request to be submitted, reviewed and approved, and tested. URE1 retained all documentation in the change management system.

URE1 applied several patches to all its PACS production servers without following the documented URE1 change management process. These PACS servers controlled all URE1 PSPs.

SERC determined that URE1 was in violation of CIP-006-1 R1.8 because it failed to afford its PACS devices the protections specified in: 1) CIP-007 R1 by failing to adequately or fully test significant changes to PACS devices to ensure there were no adverse effects on existing cybersecurity controls; 2) CIP-007 R3 by failing to assess a security patch for certain PACS components within 30 days of release; 3) CIP-007 R5 by failing to properly manage a shared account for the PACS; and 4) CIP-003 R6 by failing to follow its change management procedures when implementing a change to all its PACS production servers.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a serious or substantial risk. Specifically, the PACS components are essential to maintaining URE1's CCAs in a physically secure state.

Regarding testing, the repeated failure to adequately test changes prior to production deployment, pursuant to CIP-007 R1, increased the risk that the change might result in the inoperability of PACS components as the result of unanticipated file or code corruption or conflicts, and/or the altering of security controls in the environment. Such effects could have made the PACS more susceptible to malicious attacks that could have resulted in the inoperability of PACS components or unauthorized physical access to CCAs. However, the PACS readers would have continued to restrict access based on local memory stored on the readers, even if the PACS servers were disabled.

Regarding the database server patch, URE1's failure to timely assess a security patch pursuant to CIP-007 R3 increased the risk that an attacker could use a vulnerability to compromise the PACS database servers and give access rights to individuals without authorization or disable the PACS database servers. However, the primary facility PSP was manned 24 hours a day, seven days a week, making undetected intrusion into that area difficult. All PSPs had video cameras at the access points, which would allow for identification of any unauthorized intruders. In addition, if the PACS database servers were completely disabled without adding access rights for unauthorized individuals, the door readers and PACS control panels would have relied on internal memory until the databases were restored.

The internal memory would have limited access to those previously authorized for physical access to the PSPs. Finally, the PACS database server was protected behind corporate firewalls.

Regarding the shared account, URE1's failure to secure a shared account with read-only privileges pursuant to CIP-007 R5 increased the risk that unauthorized users might be able to obtain PACS access log information. However, even if the account had been compromised, an attacker would have only been able to obtain PSP access logs in read-only format. The account would not have permitted the modification of any PACS permissions or component operations. In addition, URE1 implemented a solution that required two-factor authentication for PACS system access.

Regarding the change management procedures, URE1's failure to follow the change management procedures pursuant to CIP-003 R6 could have resulted in the degradation of cybersecurity controls because of the installation of unapproved and untested patches. However, the patches had been assessed, tested, and approved for deployment on the corporate network and had also been assessed and approved for the additional testing required before they could be deployed to the PACS devices. The patches were in place for less than 14 days before discovery. The untested patches had been tested and deployed in non-critical systems without incident. Subsequent testing found that the untested and deployed patches did not affect the existing cybersecurity controls on the PACS.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. develop a new PACS test plan that will replace the existing PACS test plan. The new PACS test plan clearly identified the steps required to ensure changes to the PACS system do not adversely affect existing cybersecurity controls;
2. conduct training session with testing team members on the new PACS test plan;
3. execute the new PACS test plan against the production baseline and remediate any new potential violations discovered. If any were discovered, an email notification would be sent to SERC;
4. revise its CIP-007-3 R3 procedure as required by CIP-006-3 R2.2 to accurately document the processes supporting security patch management for the PACS;
5. provide training for individuals affected by the CIP-007 R3 procedural change;
6. assess missing security patch;
7. change the PACS shared database password;

8. revise its CIP-007 R5 procedure to include a process for coordinating the quarterly review of all accounts with access to the PACS;
9. provide training for individuals affected by the CIP-007 R5 procedural changes;
10. revoke the shared account access from the PACS environment;
11. apply patches in question to the PACS quality assurance servers and test;
12. provide training to the patching administration group to raise awareness that in the event technical issues occur, all patching of PACS servers would be halted until technical issues are resolved;
13. determine potential sources of failure in PACS change control and configuration management processes; and
14. develop and implement an action plan based on the results of the analysis of potential sources of failure.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (SERC2013012244)

SERC sent URE2 an initial notice of a Compliance Audit. Following the notice, URE2 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8.

URE2 failed to afford Cyber Assets used in the PACS for the PSPs the protective measures specified in CIP-007-1 R1, specifically the testing of cybersecurity controls prior to implementing significant changes.

URE2 discovered 64 instances where PACS cybersecurity controls were not tested prior to implementation into production. There were 22 instances where URE2's test plans called for testing to ensure the devices still functioned as expected but did not call for testing for any changes to the existing cybersecurity controls. There were nine instances where URE2 failed to implement the cybersecurity controls portion of the existing test plan. There were 28 instances where URE2 failed to test any cybersecurity controls on several failover PACS servers because personnel failed to recognize the servers were PACS devices. Finally, there were five instances where URE2 failed to document that any required testing had been conducted.

In addition, URE2 failed to afford PACS devices the protective measures specified in CIP-007-1 R3 by failing to assess a security patch for certain PACS components within 30 days of release. URE2 identified a missed assessment of a database security patch that was released. This was the only missed PACS database server patch, and it only applied to two PACS database servers, consisting of a primary server and a standby server.

Finally, URE2 discovered a single shared account with read-only access to the PACS that was not afforded the protective measures specified in CIP-007-1 R5. This specific account was established on the PACS database prior to the date of mandatory compliance so that individuals could run nightly reports that were used to manage and review access rights to the URE2 PSPs. Although this shared account was included in quarterly reviews, it was not afforded the protective measures required for shared accounts due to confusion between two teams regarding who was responsible for management of the account.

SERC determined that URE2 was in violation of CIP-006-1 R1.8 because it failed to afford its PACS devices the protections specified in: 1) CIP-007-1 R1 by failing to adequately or fully test significant changes to PACS devices to ensure there were no adverse effects on existing cybersecurity controls; 2) CIP-007 R3 by failing to assess a security patch for certain PACS components within 30 days of release; and 3) CIP-007 R5 by failing to properly manage a shared account for the PACS.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 executed an out-of-cycle RBAM and determined it had no CCAs.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the PACS components are essential to maintaining URE2's CCAs in a physically secure state.

Regarding testing, the repeated failure to adequately test changes prior to production deployment pursuant to CIP-007 R1 increased the risk that the change might result in the inoperability of PACS components as the result of unanticipated file or code corruption or conflicts and/or the altering of security controls in the environment. Such effects could have made the PACS more susceptible to malicious attacks that could have resulted in the inoperability of PACS components or unauthorized physical access to CCAs. However, the PACS readers would have continued to restrict access based on local memory stored on the readers, even if the PACS servers were disabled.

Regarding the database server patch, the failure to timely assess a security patch pursuant to CIP-007 R3 increased the risk that an attacker could have used a vulnerability to compromise the PACS database servers. The compromise of PACS database servers could have given access rights to

individuals without authorization or allowed individuals the ability to disable the PACS database servers. However, all PSPs had video cameras at the access points, which would have allowed for identification of any unauthorized intruder. In addition, if the PACS database servers were completely disabled without adding access rights for unauthorized individuals. The door readers and PACS control panels would have relied on internal memory until the databases were restored, which would limit access to those previously authorized for physical access to the PSPs. Finally, the PACS database server was protected behind corporate firewalls.

Regarding the shared account, the failure to secure a shared account with read-only privileges pursuant to CIP-007 R5 increased the risk that unauthorized users might be able to obtain PACS access log information. However, even if the account had been compromised, an attacker would only be able to obtain PSP access logs in read-only format. The account would not have permitted the modification of any PACS permissions or component operations. In addition, URE2 implemented a solution that required two-factor authentication for PACS system access.

URE2's Mitigation Plan to address this violation was submitted to SERC.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE2 certified that the above Mitigation Plan requirements were completed. SERC verified that URE2's Mitigation Plan was complete.

CIP-006-1 R3 (SERC2013012490 and SERC2013012495)

SERC sent the UREs an initial notice of a Compliance Audit. Following the notice, URE1 and URE2 submitted Self-Reports to SERC stating that each was in violation of CIP-006-1 R3.

Both entities had failed to retain evidence to demonstrate that they had implemented immediate human observation of PSP access points during PACS or communication outages.

The UREs' procedures required security personnel to notify the Critical Asset owner where an affected PSP existed of planned or unplanned outages of the PACS or the PACS communications network. The procedure also stated that the Critical Asset owner would be responsible for monitoring and controlling access of all authorized and unauthorized personnel.

URE1 had 365 unplanned communication outages that lasted between 15 minutes and three hours, 22 communication outages that lasted between three to six hours, 26 communication outages that lasted

between six and 24 hours, and three communication outages that lasted more than 24 hours. All the unplanned outages were due to various technical issues resulting from service provider issues or weather events.

URE2 had 84 unplanned communication outages that lasted between 15 minutes and three hours, 13 unplanned communication outages that lasted between three to six hours, ten unplanned communication outages that lasted between six and 24 hours, and three unplanned communication outages that lasted more than 24 hours. All the unplanned outages were due to various technical issues resulting from service provider issues or weather events.

Combined, the entities had planned 13 PACS server outages, for server updates, that lasted between 15 minutes and three hours.

All outages were documented by security. Planned outages were documented as change order tickets, and unplanned outages were documented in a manual communication error log. Security also maintained a manual call log to document the call to the Critical Asset owner regarding the PACS outages.

However, neither URE1 nor URE2 was able to provide any evidence that demonstrated that the manual monitoring occurred when the Critical Asset owner was notified of planned or unplanned outages. This was due to the entities' failure to define adequately the meaning of "immediate" review in procedural documentation. Further, the entities failed to relay clearly the necessity of an "immediate" response to personnel responsible for monitoring the physical access points in the event of an outage of automated controls.

SERC determined that URE1 and URE2 were in violation of CIP-006-1 R3 because they failed to retain evidence to demonstrate that they had implemented human observation of PSP access points during PACS or communication outages.

SERC determined the duration of the violations to be from the date the Standard became mandatory and enforceable on URE1 and URE2 until URE1 completed its Mitigation Plan, and until URE2 removed all remote routable protocols to its Critical Assets leaving them with no CCAs.

SERC determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the UREs' failure to review unauthorized access attempts immediately could have allowed an unauthorized individual to gain access undetected during an outage, and not be detected until the outage concluded. However, the UREs supplied evidence to demonstrate that both planned and unplanned outages had been logged, and that facility managers of

the impacted PSPs were contacted regarding the outage. CCAs contained within the PSP affected by the PACS outage were protected by an intrusion detection system that was configured to alert the UREs' personnel to any unauthorized electronic access attempts occurring locally at the implicated machine.

URE1's and URE2's Mitigation Plans to address these violations were submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. define "immediate" and document the approach to ensure unauthorized access attempts are immediately assessed during PACS or communication outages;
2. revise the corporate physical security procedure to document sufficient technical and procedural controls to immediately review unauthorized access attempts during PACS or communication outages; and
3. implement and communicate procedural changes to personnel responsible for implementing the revised corporate security physical security procedure.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE1 and URE2 certified that the above Mitigation Plans requirements were completed. SERC verified that URE1's and URE2's Mitigation Plans were complete.

CIP-006-3c R5 (SERC2013011763)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-3c R5. URE1 failed to review immediately an unauthorized access attempt alarm on one of its PSPs.

The URE1 security console received a "door open too long" alarm annunciator for a secured door at one facility. The security officer on duty acknowledged this alarm, but the security officer failed to follow URE1's procedures and did not respond or facilitate a response immediately to investigate the cause of the alarm. Approximately four hours later, an employee noticed the door at issue was open slightly and immediately left a voice message for the compliance program manager. This employee also assessed the door to determine why it was not closing and made the necessary repairs in order to get the door functioning properly and re-secured.

The compliance program manager returned to the office and received the message from the employee who discovered the door issue and repaired it. The compliance program manager notified corporate security, which investigated and determined, through review of the video footage, that there were no unauthorized access attempts during the approximately 4 hours that the door was damaged and unsecured.

SERC determined that URE1 was in violation of CIP-006-3c R5 because it failed to review immediately an unauthorized access attempt alarm received from the alarm on one of its PSPs.

SERC determined the duration of the violation to be from when URE1 corporate security received a door alarm for the facility and failed to respond immediately, through when a URE1 employee secured the door.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to investigate the alarm immediately could have allowed an intruder to gain physical access to CCAs for an extended period without being challenged, potentially giving an intruder time to manipulate or destroy CCAs.

The potential risk of the violation was mitigated by several factors. The PSP door at the facility is in a cardkey access-controlled area, which is within an access-controlled building that is manned 24 hours a day, seven days a week by onsite security personnel. The PSP door is monitored by closed circuit television cameras, which are recorded for investigative purposes. Review of the video found no attempts at unauthorized access during the violation. Lastly, the Cyber Assets contained within the PSP had an intrusion detection system running to alert URE1 personnel to any unauthorized electronic access attempts on the devices, in the case that an intruder attempted to log-on to a device from inside the PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. secure the bolt on the automatic door;
2. terminate the security officer on duty;
3. ensure the understanding of the policy and procedure between the manager of the security team and the supervisor of the security team through a meeting with the security team to discuss areas of concern; and

4. create a NERC/Regulated desk in the new security team. This desk would focus on creating and delivering comprehensive training to security team staff, managing and responding to all access control issues at NERC CIP sites, and ensuring a clear understanding of security team operating processes and procedures.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R1 (SERC2013012486)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R1.

URE1 had procedures that lacked sufficient detail to ensure significant changes to existing Cyber Assets within the ESP did not affect existing cybersecurity controls.

During an internal assessment, URE1 identified a deficiency in its testing procedures. Although the URE1 procedures called for testing to occur whenever there was a security patch deployed, the procedures did not address changes to software, version upgrades, or new applications. The procedural guidance focused primarily on the review of ports and services specifically after a security patch deployment. URE1 also omitted testing of significant changes to ensure that those changes did not affect existing cybersecurity controls such as malware prevention software, account management, and security status monitoring. Lastly, the procedure did not specify how testing results should be documented.

SERC determined that URE1 was in violation of CIP-007-1 R1 because it failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 conducted cybersecurity controls testing on each affected Cyber Asset.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE1's failure to test security controls after significant changes could have permitted implemented changes to eliminate or degrade existing security controls and permit unauthorized access to CCAs, resulting in available attack vectors to CCAs, which could have permitted compromise of the CCAs.

However, URE1 did ensure that significant changes did not change the enabled ports and services. In addition, all Cyber Assets were secured within ESPs and PSPs, and the ESPs were protected by an intrusion prevention system.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. review its guidelines for test procedures and develop a list of controls to be tested by asset type;
2. update a test procedure to include a comprehensive list of cybersecurity controls;
3. update a test procedure to ensure the test results are documented for each significant change;
4. provide training for the individuals affected by the procedural changes made to the test procedure; and
5. perform a cybersecurity controls test on each of the managed Cyber Asset types.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R2.2 (SERC2013012487)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R2. URE1 failed to implement sufficiently its process to ensure that only those ports and services required for normal and emergency operations were enabled.

While conducting an internal compliance review, URE1 discovered that there were ports and services enabled on multiple CCAs and non-critical Cyber Assets within the ESP that were not documented as being required for normal or emergency operations.

Approximately 15% of the Cyber Assets had several hundred ports and services that were enabled but without supporting documentation for why the ports and services were required. URE1 had identified undefined ports and services as action items to address in its annual CVAs, but due to deficiencies in its ports and services procedure, these ports and services were not disabled or documented as being necessary for normal or emergency operations. URE1 concluded the root cause of the violation was a human performance issue where support personnel failed to take the remedial actions required in its

systems security management procedure to disable unused ports and services where necessary and document the results.

SERC determined that URE1 was in violation of CIP-007-1 R2.2 because it failed to disable ports and services not required for normal and emergency operation.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 documented the need for the enabled ports and services required for normal or emergency operations and disabled the ports and services that were not required for normal or emergency operations.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE1's failure to document the need for enabled ports and services and its failure to disable unneeded ports and services for over several years gave individuals a protracted opportunity to exploit or degrade CCAs, and potentially cause URE1 to lose its visibility of, or control over, its portion of the BPS. Moreover, the failure of URE1 to remediate the port and service issues identified during its annual CVAs is indicative of further weaknesses in URE1's documentation and justification of ports and services that were enabled. However, CCAs and non-critical Cyber Assets were secured within an established ESP, which included an intrusion prevention system.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. conduct a review session for the relevant group on the CIP-007 R2 procedure;
2. review and document the justification of the "not defined" or "unknown" ports and services;
3. disable any unnecessary ports and services;
4. review and evaluate the CIP-007 R2 procedure to determine if any process changes were required and update the CIP-007 R2 procedure; and
5. provide training for the individuals affected by the procedural changes to the CIP-007 R2 procedures.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R3 (SERC2013012532)

URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R3. URE1 failed to review applicable software security patches for all Cyber Assets within the ESP within 30 days of availability and failed to document adequately the assessment and implementation of security patches.

SERC determined that URE1 was in violation of CIP-007-1 R3 because it failed to review applicable software security patches for all Cyber Assets within the ESP within 30 days of availability and failed to document adequately the assessment and implementation of security patches. The associated Cyber Assets included communication processors, EMS devices, workstations, and servers.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE1 until URE1 implemented an interim solution for tracking the implementation of security patches.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to document adequately the application of security patches or the decision not to apply security patches where appropriate increased the risk that URE1 may have failed to identify patching gaps. Additionally, the failure to timely assess patches affected various CCAs and non-critical Cyber Assets and increased the time those Cyber Assets were exposed to vulnerabilities. These failures could allow a malicious actor to use previously identified vulnerabilities to disrupt URE1's ability to monitor and control its portion of the BPS.

However, the communication processors were isolated to communications originating within the URE1 EMS, and they were located in physically secured facility environments. Regarding the EMS devices, the EMS ESPs were monitored by network-based intrusion prevention. The workstations were deployed with host-based intrusion detection systems. One patch affected seven Cyber Assets and a second patch was assessed three days past the permitted 30-day assessment window. In addition, the ESP network was segregated from the enterprise network. The URE1 EMS had its own active directory that is separate from the enterprise active directory. All of the Cyber Assets involved in this violation are secured within an established ESP and PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. create a requirements list from all the groups involved in the patch management process to ensure the implementation of security patches or upgrades were sufficiently documented;

2. implement an interim solution for tracking the implementation of patches;
3. implement the interim solution as a permanent solution for tracking the implementation of changes, and then document and communicate procedural changes in support of the permanent solution;
4. apply all applicable security patches for the missed assessments;
5. complete and document all applicable patch assessments for the specific product;
6. update the CIP-007 R3 procedure to require the assessor to review their software inventory for any manual patch discovery processes. Reviewing the software inventory as part of the discovery process ensures that all security patch alerts or advisories are tracked and assessed for all applicable software versions;
7. provide training for the individuals affected by the updated CIP-007 R3 procedure;
8. update the CIP-007 R1 procedure to address steps for adding, incrementing, or removing software versions to the patch assessment process;
9. provide training for the individuals affected by the updated CIP-007 R1 procedure;
10. remap all instances of the affected software application to correct entries with a third-party vendor, which was monitoring a different version of the software;
11. assess patches missed due to vendor configuration error;
12. coordinate with the third-party vendor to look for other instances of incorrect associations or dead links;
13. assess patches missed due to the systems failure;
14. install monitoring and notifications to alert on failed application conditions relating to the task creation and initial email notification functions;
15. survey industry peers to look for patch management best practices that could be applied;
16. perform a review of all automated functions of the patch management alerting process and ensure system personnel are promptly notified of the failure of any function that could impact compliance;
17. analyze all potential patch management sources of failure across all accountable groups; and
18. if necessary, execute an action plan to address new potential sources of failure or best practices not previously addressed.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R6 (SERC2013012243)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R6.

URE1 failed to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP.

URE1's procedure for security monitoring required URE1 to monitor CCAs for attempts to connect to unauthorized ports and services, however the procedure lacked sufficient detail to meet the requirements of CIP-007 R6.

URE1 also did not proactively review its system for potential Cyber Security Incidents or events related to cybersecurity that might not produce functional abnormalities. Instead, URE1 operationally depended on the system operators and their experience and knowledge to detect and alert system administrators of any functional abnormalities.

SERC determined that URE1 was in violation of CIP-007-1 R6 because it failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 implemented an automated process to monitor and alert on system events related to cybersecurity.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE1's failure to monitor for events related to cybersecurity could have permitted a malicious actor to gain access to or compromise CCAs, thereby threatening URE1's visibility over, or control of, its portion of the BPS. However, URE1 had trained system operators on shift 24 hours a day, seven days a week who monitored the system for system performance issues. URE1 utilized an intrusion prevention system within the secured ESPs. All involved CCAs were secured within an ESP and PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. implement a security information and event management (SIEM) system to monitor and alert on system events related to cybersecurity for Cyber Assets within the ESPs;
2. update CIP-007 R6 procedure to reflect the new SIEM system and specify and require documentation necessary to demonstrate compliance with CIP-007 R6;
3. provide training to individuals affected by CIP-007 R6 procedural changes;
4. update change management procedures to ensure all Cyber Assets are communicating with the SIEM system, where technically feasible; and
5. provide training to individuals affected by change management procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R8.3 (SERC2013012489)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R8.3.

URE1 failed to have sufficient detail in its internal procedures to ensure its staff adequately performed a review of the controls for default accounts during CVAs.

URE1's CVA procedure required the annual review of default accounts, evaluation of the results, and that the remediation plan for any issues discovered be documented and tracked through completion.

Through an internal assessment of its CVA procedure, URE1 determined that the existing CVA procedure, although requiring the review of all default accounts, did not contain adequate detail on how to conduct a review of controls for default accounts.

URE1's CVA remediation plans documented that a scan for default applications and system accounts and log-ins was conducted for a period of two years. The remediation plans also documented that the scan found no default accounts enabled. URE1's CVA remediation plan for the following year did not document that a scan for default user accounts had been conducted.

URE1 reviewed the CVA procedures for all other areas and found no other deficient CVA processes.

SERC determined that URE1 was in violation of CIP-007-1 R8.3 because it failed to have sufficient detail to perform an adequate review of the controls for default accounts. The existing procedure did not address the controls associated with default accounts.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE1's failure to establish sufficient procedures to ensure adequate evaluation and controls around default accounts during annual CVAs could have permitted a malicious individual to exploit an existing default account, gain access and control of CCAs, and eliminate or corrupt data being used to make operational decisions. However, URE1 did include a review of enabled ports and services in its annual CVAs and had documented action plans to remediate any issues that were discovered during the CVAs. All Cyber Assets were secured with an ESP and a PSP, and the network was monitored via network- and host-based intrusion detection systems. Security status monitoring of Cyber Assets within the ESP indicated no unauthorized or malicious activity during the violation.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. update its CIP-007 R8.3 procedure to include all controls for default accounts;
2. provide training for the individuals affected by the procedural changes made to the CIP-007 R8.3 procedure;
3. obtain asset access control lists to review the population of default accounts and their available controls; and
4. execute updated CIP-007 R8.3 procedure to include a review of all default accounts and their controls.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-009-1 R1 (SERC2013012491)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-009-1 R1. URE1's recovery procedures lacked sufficient detail to recover all CCAs.

URE1 implemented two separate recovery plans for its CCAs. The separate plans addressed CCAs associated with different groups.

URE1 completed an internal review of the first plan. It discovered that the existing recovery procedures were insufficient to ensure a complete recovery from the loss of CCAs. SERC reviewed the first plan and determined that it did not provide details on how to manage properly hardware changes or upgrades resulting from a recovery, and it failed to define roles and responsibilities of responders and response actions to events of varying duration and severity. URE1 maintained a supplemental document detailing the required steps for documenting, testing, and updating hardware changes, but this hardware change procedure was not linked to or referenced from the first plan.

Regarding the second plan, SERC determined that it was written as a higher-level disaster recovery plan of facilities and systems, and failed to address the recovery of the specific Cyber Assets in service within the second group, define the roles and responsibilities of responders, and specify the required actions in response to events of varying severity and duration. Nevertheless, the second plan was supplemented by a recovery process document that addressed the replacement of CCAs and provided instructions to recover Cyber Assets and return them to service using previously approved settings. The recovery process document also referenced a site where a replacement Cyber Asset could be obtained, but did not provide any detail on the systems or tools and applications that should be used to recover the replacement Cyber Asset to return to normal operations.

SERC determined that URE1 was in violation of CIP-009-1 R1 because its recovery procedures lacked sufficient detail to recover all CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 successfully recovered CCAs throughout the violation period without issues, depending on the skill and experience of the technicians and system operators. URE1 conducted successful weekly failover of the systems to back-up redundant systems, which would have been available in the event of a prolonged recovery of a CCA, or in the event of a more widespread event

affecting multiple CCAs. The response personnel for URE1 were trained and aware of the existing procedures and were able to respond to and recover CCAs based on their experience and knowledge.

URE1's Mitigation Plan to address this violation was submitted to SERC. URE1's Mitigation Plan required URE1 to:

For The First Plan

1. assess the CIP-009 procedures and evaluate the steps to properly perform a technical recovery of each CCA type;
2. update the CIP-009 procedures incorporating changes based on the assessments completed for each CCA type;
3. approve and distribute updated CIP-009 procedures;

For The Second Plan

4. review and enumerate the Cyber Asset types which needed additional details added to the existing CIP-009 technical recovery procedure;
5. create a schedule to update procedures based on the list of Cyber Asset types that needed additional details added to the CIP-009 recovery procedures;
6. update procedures for half of the Cyber Asset types based on the schedule previously developed; and
7. complete procedure updates for the remaining Cyber Asset types.

URE1 certified that the above Mitigation Plan requirements were completed.

SERC verified that URE1's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred twenty thousand dollars ($120,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE1 and URE2 had prior violation history, which was considered as an aggravating factor in the penalty determination;
2. the UREs had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor;

3. URE1 self-reported the violation of CIP-003-3 R6. The UREs did not receive mitigating credit for self-reporting the remaining violations because the Self-Reports were submitted after receiving notice of an upcoming Compliance Audit;
4. the UREs were cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of SERC2013012483, SERC2014013371, SERC2013012237, SERC2013011770, SERC2013012498, SERC2013012488, SERC2013012496, SERC2013011754, SERC2013012240, SERC2013011761, SERC2013012490, SERC2013012495, SERC2013011763, SERC2013012486, SERC2013012532, SERC2013012243, SERC2013012489, and SERC2013012491 posed a minimal or moderate risk. The violations of SERC2013012242, SERC2013012244, and SERC2013012487 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
7. as explained in more detail in Attachment A to the Settlement Agreement, in addition to paying the monetary penalty, the UREs has completed or has committed to complete the following above-and-beyond mitigating actions, which SERC took into consideration when assessing the proposed penalty:
    a. UREs have hired additional full-time staff resources and converted some contractors to permanent positions, with some of the additional personnel dedicated to NERC CIP compliance and activities focused on the UREs' CIP Version 5 implementation. Although the remaining additional personnel are not dedicated compliance resources, the UREs report that the extra staff has allowed existing compliance resources to focus more time on improving their controls and accurately executing existing compliance processes.
    b. UREs have provided NERC CIP personnel with basic human performance training and personnel with advanced human performance training. UREs also provided personnel with root cause analysis training to support cause identification with all future Self-Report efforts. The cost of this training was approximately $50,000.
    c. UREs have implemented firewall analyzer software that actively monitors UREs' firewalls protected pursuant to the CIP Standards. Implementation of the firewall analyzer software cost approximately $485,000.
    d. UREs have conducted other mitigation efforts outside of its formal Mitigation Plans for CIP-004 R4, CIP-006-3 R2.2, CIP-006-3 R5, CIP-007 R1, and CIP-007 R3 that SERC considered to be mitigating factors in the penalty determination.
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred twenty thousand dollars ($120,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 18, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred twenty thousand dollars ($120,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Marisa A. Sifontes* General Counsel Drew R. Slabaugh* Legal Counsel Rebecca A. Lindensmith* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 414-5244 (704) 414-5230 (704) 357-7914 – facsimile msifontes@serc1.org dslabaugh@serc1.org rlindensmith@serc1.org James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Andrea B. Koch* Director of Compliance and Analytics SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior
Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entities
SERC Reliability Corporation

Attachments

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2014

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of one hundred twenty thousand dollars ($120,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Total Penalty
WECC2013012030	CIP-002-1	R3	Lower/ Severe	$120,000
WECC2013012032	CIP-004-1	R2; R2.2	Medium/ Severe	
WECC2013012685	CIP-004-1	R4; R4.1	Lower/ High	

NERC Violation ID	Reliability Standard	Req.	VRF/ VSL*	Total Penalty
WECC2013012326	CIP-005-1	R1; R1.5	Medium/ Severe	$120,000
WECC2013012935	CIP-005-1	R2; R2.1	Medium/Severe	
WECC2013012937	CIP-005-3a	R4	Medium/Severe	
WECC2013012327	CIP-006-1	R1; R1.8	Medium/ Severe	
WECC2013012946	CIP-006-3c	R8	Medium/Severe	
WECC2013012939	CIP-007-1	R5; R5.2	Lower/ Severe	
WECC2013012940	CIP-007-1	R6; R6.1	Medium/ Severe	
WECC2013012938	CIP-007-3a	R8; R8.4	Medium/ Severe	
WECC2013012033	CIP-009-1	R1	Medium/ Severe	
WECC2013012034	CIP-009-2	R4	Lower/ Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-1 R3 (WECC2013012030)

URE submitted a Self-Certification stating that it was in violation of CIP-002 R3. URE failed to include three Cyber Assets on its list of Critical Cyber Assets (CCAs). The purpose of the devices is to convert remote terminal unit (RTU) data from transmission control protocol/internet protocol into serial communications data and back. The root cause of the violation was determined to be human error, related to URE's initial assessment that the devices did not have routable protocol.

WECC determined that URE had a violation of CIP-002-1 R3 for failing to include three Cyber Assets on its list of associated CCAs essential to the operation of the Critical Asset.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). All of the devices were located inside a Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP). Physical and logical access was limited to only authorized URE staff with the appropriate authorizations to access each device.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to add the three Cyber Assets to its Cyber Asset hardware list and clarify the specific asset types in the list.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-004-1 R2; R2.2 (WECC2013012032)

URE submitted a Self-Certification to WECC stating that it was in violation of CIP-004 R2. URE failed to review its cybersecurity training program for one year. In addition, URE's program did not include the items required by CIP-004-1 R2.2.1-R2.2.4. Specifically, URE's training material did not specifically train individuals on: (i) the proper use of CCAs; (ii) physical and electronic access controls to CCAs; (iii) the proper handling of CCA information; and (iv) action plans and procedures to recover or re-establish CCAs and access thereto following a Cyber Security Incident. While WECC determined that this

information was covered in URE's separate awareness training, it was not included as part of URE's cybersecurity training program as required by the Standard.

WECC determined that URE had a violation of CIP-004-1 R2 for failing to review its cybersecurity training program annually and for failing to include all of the required topics.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE reviewed its training program in the year before and the year after the violation year. URE conducted training for all personnel who had authorized unescorted logical or physical access. The cybersecurity training program familiarized personnel with the language and procedures of the CIP standards. While the training program did not meet all of the requirements of CIP-004 R2, it did include training on the CIP-002 through CIP-009 standards and URE's policies and procedures. Additionally, although URE's cybersecurity training did not specifically cover all required areas, URE's additional cybersecurity awareness training, which was provided upon initial implementation of the CIP program, did cover these areas. Further, URE conducted quarterly awareness activities to reinforce security practices.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update the training program document to reflect more accurately the training being conducted;
2. review and incorporate the cybersecurity training presentation; and
3. conduct training for all personnel with unescorted logical or physical access using a revised and formalized cybersecurity awareness training presentation which includes all the required components of the Standard.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-004-1 R4; R4.1 (WECC2013012685)

URE submitted a Self-Report stating that it was in violation of CIP-004-1 R4. WECC conducted a Compliance Audit of URE (Compliance Audit). During the Compliance Audit, WECC staff reviewed the scope of URE's Self-Report.

WECC determined that URE failed to maintain its list of personnel with authorized cyber access to CCAs in two instances. In the first instance, URE updated its list 21 days prior to granting logical access to an employee. URE updated its list within seven days of access being authorized, not access being granted. In the second instance involving a different employee, URE updated its list one month after logical access was granted.

WECC determined that URE had a violation of CIP-004-1 R4 for failing to maintain its list of personnel with authorized Cyber Assets to CCAs and update the list within seven calendar days of any change.

WECC determined the duration of the violation for the first instance to be from the date URE changed its access list prior to access being granted through the date URE granted access to that employee. WECC determined the duration of the violation for the second instance to be from the eighth day after URE granted access to the employee through the date URE updated its access list to reflect this change.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Both individuals who were granted access received CIP training and had completed Personnel Risk Assessments. The issue was limited to the failure to update the list in a timely manner; no access to CCAs was granted to unauthorized personnel. Both individuals had "need to know" local access to CCAs.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. modify the steps it uses to grant or revoke access to include additional tracking and controls; and
2. confirm that access lists were current.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-005-1 R1; R1.5 (WECC2013012326)

WECC contacted URE to discuss URE's Self-Certifications of CIP-009 R1 and CIP-009 R4 (WECC2013012033 and WECC2013012034, respectively). During this discussion, URE stated that the scope of these violations included four devices used in the electronic access control and monitoring (EACM) of two ESPs. The EACM devices consisted of modems, servers, and firewalls.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to afford all of the protections required by CIP-005-1 R1.5 (specifically, CIP-003 R4, CIP-009 R1, and CIP-009 R4) to EACM devices used to monitor two ESPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the EACM devices within a PSP. Access to the PSP was restricted, actively monitored, and logged. Only authorized individuals were permitted to access the PSP. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. URE had backup and restore procedures in place for Windows devices, and it was recording tape backups regularly.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. revise its information protection plan;
2. classify all documents as required by the plan that were not previously marked as information associated with CCAs; and
3. update its recovery plan to include EACM devices, including backup media.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-005-1 R2; R2.1 (WECC2013012935)

During the Compliance Audit, WECC discovered that URE failed to provide required access point security controls for two access points to the ESPs in violation of CIP-005 R2. Two servers did not

provide the ability to specify explicit access permission for all communication at these access points. Further, one of the access points did not provide strong network separation between two ESPs and the physical security network.

WECC determined that URE had a violation of CIP-005-1 R2 for failing to ensure that the two access points to the ESP used an access control model that denied access by default, such that explicit access permissions must be specified.

WECC determined the duration of the violation to be from when one of the two access points was installed through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE locked down the devices to disable routing across its interfaces. The devices had antivirus and other CIP-007 protections, such as patching and logging. The devices were performing real-time logging and monitoring of all traffic. The devices were protected by firewalls with explicit rules for all traffic. The devices were within a defined PSP. There was no interactive access into any ESP or across the access point boundary, except emergency vendor modem access with defined manual procedures to enable this access. Further, the access points at issue were used only to collect logs and generate alerts from ESP devices and physical access control system (PACS) devices.

URE's Mitigation Plan to address this violation was submitted to WECC stating it had been completed.

URE's Mitigation Plan required URE to:

1. move the two devices out of the ESP and into a demilitarized zone with explicit access lists to allow proper network traffic flow for collection of security events from ESP CCA devices; and
2. reclassify the devices as monitoring devices of the ESP.

CIP-005-3a R4 (WECC2013012937)

During the Compliance Audit, WECC discovered that URE failed to conduct an annual Cyber Vulnerability Assessment (CVA) for one access point in violation of CIP-005-3a R4. URE failed to include the configuration information for a dial-up accessible modem to the third party conducting the annual CVAs for URE. WECC also discovered that URE failed to document the execution status of its action plan to remediate or mitigate vulnerabilities identified in the CVAs for two calendar years for all four of its access points.

WECC determined that URE had a violation of CIP-005-3a R4 for failing to perform a CVA for one access point and for failing to document the execution status of the action plan to remediate or mitigate vulnerabilities in the CVA for four access points.

WECC determined the duration of the violation to be from the last date in the first calendar year it could have complied with the annual CVA requirement through the last date in the second calendar year it could have complied with the annual CVA requirement.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture designed to prevent malicious cyber attacks. Specifically, URE used various physical and logical cybersecurity controls, physical security mechanisms (special locks and closed circuit television), additional firewalls, vulnerability scanning tools, and internal cybersecurity controls.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. remove the modem from service and the CIP asset inventory; and
2. conduct the annual CVA to get a new baseline of action plans for the devices, and create additional tracking mechanisms to ensure the action plans and execution status are updated.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-006-1 R1; R1.8 (WECC2013012327)

WECC contacted URE to discuss URE's Self-Certifications of CIP-009 R1 and CIP-009 R4 (WECC2013012033 and WECC2013012034, respectively). During the interview, URE stated that the scope of these violations included 10 devices used in the physical access control and monitoring of two PSPs. The devices consisted of workstations, servers, controllers, and switches.

WECC determined that URE had a violation of CIP-006-1 R1 for failing to provide several of the protections specified in R1.8 (specifically, CIP-003 R4, CIP-009 R1, and CIP-009 R4) to Cyber Assets used in the access control and monitoring of the PSPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the devices within an ESP. Access to the ESP was restricted, actively monitored, and logged. Many of the devices were redundant; failure of these devices would not affect URE's network infrastructure. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. URE had backup and restore procedures in place for Windows devices and was recording tape backups regularly.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. revise its information physical access protection plan and mark all documents as required by the plan that were not previously marked; and
2. update its recovery plan to include CIP-006 assets, including protective measures from unauthorized physical access.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-006-3c R8 (WECC2013012946)

During the Compliance Audit, WECC discovered that URE failed to implement a maintenance and testing program that ensured all of the physical security systems under Requirements R4, R5, and R6 functioned properly, in violation of CIP-006-3c R8. Specifically, URE did not conduct the testing of specified controls at each PSP access point during maintenance and testing activities. The testing included some maintenance activities, such as cleaning camera lenses and updating software, but did not include testing of door alarms, glass break sensors, or logging of alarms in the PACS system.

WECC determined that URE had a violation of CIP-006-3c R8 for failing to implement a maintenance and testing program to ensure that all physical security systems under R4, R5, and R6 functioned properly.

WECC determined the duration of the violation to be from one month past the prior audit interval through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had multiple layers of security. The PSPs were staffed at all times and/or protected by fencing. URE's contractor was performing preventative maintenance activities on a semi-

annual basis. Further, URE provided evidence showing that, as of a certain date, the physical security systems for a PSP area were tested to meet its installation requirements.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update its maintenance and testing procedure;
2. develop a checklist and sign-off sheet; and
3. schedule maintenance with vendor to conduct maintenance as prescribed in new plan.

CIP-007-1 R5; R5.2 (WECC2013012939)

During the Compliance Audit, WECC discovered that URE was in violation of CIP-007 R5. URE failed to remove, disable, or rename the built-in Windows administrator account on one PACS device as required by R5.2.1.

WECC determined that URE had a violation of CIP-007-1 R5 for failing to implement a policy to remove, disable, or rename a built-in administrator account on a PACS device.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE deactivated the administrator account during the Compliance Audit.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This was an isolated event, and the account did not have a default password assigned. URE had changed the password at least once, but not annually, after enabling the account. Further, URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and a security events management system.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to disable the account.

URE certified that the above Mitigation Plan requirement was completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-1 R6 (WECC2013012940)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007 R6. URE failed to provide sufficient evidence of security event monitoring for one CCA, a video display board.

WECC determined that URE had a violation of CIP-007-1 R6 for failing to implement and document the organizational processes and technical and procedural mechanisms for monitoring system events related to cybersecurity for one CCA within the ESP.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation was isolated and affected only one device. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and a security events management system.

URE's Mitigation Plan to address this violation was submitted to WECC stating it had been completed.

URE's Mitigation Plan required URE to:

1. monitor the video board device; and
2. provide evidence of logging for 90 days.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-3a R8; R8.4 (WECC2013012938)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R8. URE failed to document the execution status columns of the action plans to remediate or mitigate vulnerabilities identified during the CVAs of all Cyber Assets within the ESP for two calendar years due to staffing shortfalls.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to document the execution status of the action plans for two CVAs.

WECC determined the duration of the violation to be from the last date in the first calendar year URE could have complied with the annual CVA requirement through the last date in the second calendar year URE could have complied with the annual CVA requirement.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms with guards, special locks, closed circuit television, and logical perimeter and internal cybersecurity controls, including firewalls, vulnerability scanning tools, and intrusion detection systems.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. conduct an annual CVA to get a new baseline of action plans for the devices; and
2. create additional tracking mechanisms to ensure the action plans and execution status are updated.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (WECC2013012033)

URE submitted a Self-Certification stating it was in violation of CIP-009 R1. URE failed to create a recovery plan for CCAs that specified the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan. In addition, WECC determined that URE's recovery plan did not address any networking CCAs or non-critical Cyber Assets.

WECC determined that URE had a violation of CIP-009-1 R1 for failing to create a recovery plan for all CCAs and for failing to ensure that the plan specified the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had vendor service agreements in place to aid in the recovery of CCAs. Many of the non-Windows devices were redundant, such that URE's business would not be impacted

by a single failure. Further, URE's information technology personnel responsible for recovery had practical knowledge of the devices and therefore had the experience to recover CCAs in the event of a Cyber Security Incident.

URE's Mitigation Plan to address this violation was submitted to WECC. URE's Mitigation Plan required URE to update its recovery plan.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-009-2 R4 (WECC2013012034)

URE submitted a Self-Certification stating that it was in violation of CIP-009 R4. URE failed to include processes and procedures for the backup and storage of information required to successfully restore network switches, firewalls, terminal servers, and control panels. Specifically, URE's backup and restore procedures did not contain sufficient detail and listed as resources only the vendor recovery documentation (however, the procedures did not provide the locations of the vendor documentation).

WECC determined that URE had a violation of CIP-009-2 R4 for failing to ensure that the recovery plan included processes and procedures for the backup and storage of information required to successfully restore CCAs.

WECC determined the duration of the violation to be from the day after WECC previously notified URE that it was compliant with the Standard through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained the devices within an ESP, access to which was restricted, actively monitored, and logged. Many of the devices were redundant; therefore, failure of these network devices would not affect URE's network infrastructure. URE had written maintenance agreements with vendors to contact URE within eight hours and restore the devices if URE encountered an issue. Further, URE had backup and restore procedures in place for Windows devices and was recording tape backups regularly.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to update its process document to include detailed steps describing how URE conducts its backup procedures.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred twenty thousand dollars ($120,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's prior violations as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. URE took voluntary corrective action to remediate this violation, which WECC considered a mitigating factor;
6. the violations posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred twenty thousand dollars ($120,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 18, 2014 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by WECC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred twenty thousand dollars ($120,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Chris Luras* Director of Compliance Risk Analysis & Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz

Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and
Senior Director of Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

December 30, 2014

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP15-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A regarding 10 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

The Spreadsheet NOP resolves 40 violations[5] of 9 Reliability Standards. In order to be a candidate for inclusion in the Spreadsheet NOP, the violations are those that had a minimal or moderate impact on the reliability of the bulk power system (BPS).

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.
[3] Attachment A is an excel spreadsheet.
[4] *See* 18 C.F.R § 39.7(c)(2).
[5] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. As designated in the attached spreadsheet, some of the Registered Entities have admitted to the violations, while the others have indicated that they neither admit nor deny the violations and have agreed to the proposed penalty as stated in Attachment A or did not dispute the violations and proposed penalty amount stated in Attachment A, in addition to other remedies and mitigation actions to mitigate the instant violations and ensure future compliance with the Reliability Standards. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

As discussed below, this Spreadsheet NOP resolves 40 violations. NERC respectfully requests that the Commission accept this Spreadsheet NOP.

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Text of the Reliability Standards at issue in the Spreadsheet NOP may be found on NERC's web site at http://www.nerc.com/page.php?cid=2|20. For each respective violation, the Reliability Standard Requirement at issue and the applicable Violation Risk Factor are set forth in Attachment A.

Unless otherwise detailed within the Spreadsheet NOP, the Registered Entities were cooperative throughout the compliance enforcement process; there was no evidence of any attempt to conceal a violation or evidence of intent to do so. In accordance with the Guidance Order issued by FERC concerning treatment of repeat violations and violations of corporate affiliates, the violation history for the Registered Entities and affiliated entities who share a common corporate compliance program is detailed in Attachment A when that history includes violations of the same or similar Standard. Additional mitigating, aggravating, or extenuating circumstances beyond those listed above are detailed in Attachment A.

Status of Mitigation[6]

The mitigation activities are described in Attachment A for each respective violation. Information also is provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[7]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order, the August 27, 2010 Guidance Order and the March 15, 2012 Compliance Enforcement Initiative Order,[8] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee. Such considerations include the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, the NERC Enforcement staff's review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the violations at issue.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[6] *See* 18 C.F.R § 39.7(d)(7).
[7] *See* 18 C.F.R § 39.7(d)(4).
[8] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Associate General Counsel and Senior Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Associate General Counsel and Senior Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

Attachment a

Spreadsheet Notice of Penalty
(Included in a Separate Document)

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY AND REGISTERED ENTITY SERVICE LIST FOR DECEMBER 2014 SPREADSHEET NOP FILING

For MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
P:651-855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Vice President of Regulatory Affairs and Enforcement
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
P:651-855-1708
se.patrick@midwestreliability.org

FOR RFC:

Robert K. Wargo*
Vice President
Reliability Assurance & Monitoring
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(216) 503-0682
(216) 503-9207 facsimile
bob.wargo@rfirst.org

Niki Schaefer*
Managing Enforcement Attorney
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(216) 503-0689
(216) 503-9207 facsimile
niki.schaefer@rfirst.org

Jason Blake*
General Counsel & Corporate Secretary
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(216) 503-0683
(216) 503-9207 facsimile
jason.blake@rfirst.org

Kristina Pacovsky*
Counsel
ReliabilityFirst Corporation
3 Summit Park Drive, Suite 600
Cleveland, OH 44131
(216) 503-0670
(216) 503-9207 facsimile
kristina.pacovksy@rfirst.org

FOR SERC:

Marisa A. Sifontes*
General Counsel
Drew R. Slabaugh*
Legal Counsel
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 494-7775
(704) 414-5244
(704) 357-7914 – facsimile
msifontes@serc1.org
dslabaugh@serc1.org

James M. McGrane*
Managing Counsel – Enforcement
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 494-7787
(704) 357-7914 – facsimile
jmcgrane@serc1.org

Andrea B. Koch*
Director of Compliance and Analytics
SERC Reliability Corporation
3701 Arco Corporate Drive, Suite 300
Charlotte, NC 28273
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

FOR WECC:

Jim Robb*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6853
jrobb@wecc.biz

Chris Luras*
Director of Compliance Risk Analysis & Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7674
(801) 883-6894 – facsimile
rarredando@wecc.biz

Attachment A-2

December 30, 2014 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
2	ReliabilityFirst Corp	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012741	CIP-003-3	R6	Lower	Severe	The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Network Consultant's failure to follow the RFC_URE1 change management process resulted in a 45-minute loss of visibility to a device . Although RFC_URE1 failed to implement its change management procedure in this instance, all other testing procedures were followed for the erroneous application of the unapproved network changes. In addition, protective relays, which do not depend on network connectivity, continued to function, and the control center was able to monitor the lines affected by the communication outage via monitoring equipment at neighboring stations. Lastly, cybersecurity logging was still occurring locally during this period and the review of the logs did not show any reportable cybersecurity incident during the noncompliance, during which time the devices on the network were isolated.
3	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013011812	CIP-006-3c	R4	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the PSP door was unsecured, it was configured to alarm when opened and was in working condition. The Cyber Assets were located within a facility that was protected by a perimeter fence that required restricted card access to enter, as well as cameras throughout the location.
4	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013012154	CIP-006-3c	R2; R2.2	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failing to remove access to and update the access lists for PSPs could have allowed unauthorized access to go unnoticed, potentially allowing malicious access. Further, failure to track and maintain a list of personnel with cyber access to PACS could have allowed individuals with cyber access to PACS to manipulate or alter physical access authorizations to Critical Cyber Assets (CCAs), either purposefully or by mistake, resulting in disruption or loss of control of the energy management system or SERC_URE1's portion of the BPS. However, neither operator account had permission levels that could affect the integrity of the CIP infrastructure. In addition, failing to assess and to implement security patches and security upgrades, where applicable, combined with the failure to document compensating measures if not installed, could have left software on the affected Cyber Assets vulnerable, increasing the risk of a cyber-attack that could result in operational impacts and potential degradation of the BPS. However, the affected Cyber Assets were behind corporate firewalls and intrusion detection and intrusion protection systems were deployed on the network. Also, the individuals in question would not have cyber access because automated processes would have removed access within 24 hours.

	L	M
1	Violation Start Date	Violation End Date
2	when RFC_URE1 failed to follow its change control and configuration management process	Mitigation Plan completion
3	when the door was left unsecure	when the door was secured
4	30 days following the first patch release	when the administrator accounts to PACS were documented

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
2	$0	Self-Report	To mitigate this violation, RFC_URE1: 1) revised its change management process to require a RFC_URE1 IT staff member to be present at the control center and deployed in the field while changes are implemented in case an outage occurs; 2) conducted training on its revised change management process for its IT personnel; 3) instituted a pre- and post-implementation peer review of significant changes to RFC_URE1's NERC CIP Networks; and 4) also updated its change request form to reflect the new, pre- and post-implementation peer review.	7/24/2013	8/13/2014	Admits
3	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Certification	To mitigate this violation, SERC_URE1: 1) locked the door and ensured it was secure; and 2) disabled the locking mechanism to prevent the ability to unlock the door.	12/5/2012	3/5/2014	Neither Admits nor Denies
4	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Report	To mitigate the first incident in this violation, SERC_URE1: 1) subscribed to an alerting feature for extended support of notifications; 2) conducted a meeting to determine the extent of condition; 3) implemented patches; and 4) updated documentation. To mitigate the second incident in this violation, SERC_URE1: 1) suspended the 1st and 2nd operator accounts; and 2) developed a security officer termination process.	9/30/2014	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
2	ReliabilityFirst considered certain aspects of the RFC_URE1's compliance program as mitigating factors. ReliabilityFirst also considered that the violation was caused by a rogue employee and did not indicate a systemic problem at RFC_URE1 such as a lack of awareness and training on RFC_URE1 change management process. ReliabilityFirst considered this fact a mitigating factor in the penalty determination. However, because RFC_URE1's failure to implement its change management procedure resulted in harm to its operations, and because RFC_URE1's initial response to the violation allowed a second failure to occur that was caused by the same employee, ReliabilityFirst determined that the violation did not qualify for Find, Fix, Track and Report (FFT) or Compliance Exception disposition. The need for a monetary penalty was eliminated by the significant credi given for RFC_URE1's timely detection, correction and reporting, and its well-established history of doing so in prior matters.
3	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
4	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
5	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013012155	CIP-005-1	R1; R1.5	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failing to properly identify access points greatly increases the risk of Critical Cyber Assets (CCAs) being compromised and rendered inoperable, which could have caused the loss of monitoring and control of numerous BPS elements. A violation of CIP-005-1 R1.5 has the potential to affect the reliable operation of the BPS by providing the opportunity for cyber intrusions to occur on CCAs located within the established ESP. However, the unidentified access points were serially connected which utilized non-routable protocols and were protected inside a Physical Security Perimeter (PSP). All personnel with access to the PSP had NERC CIP training and current personnel risk assessments. Also, SERC_URE1 had a defense in-depth strategy of protection that an intruder would have to overcome to gain access to the devices. These protections include corporate firewalls, intrusion detection systems, and intrusion prevention systems.
6	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013012520	CIP-005-3a	R1	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SERC_URE1's failure to follow its change control and configuration management processes resulted in it failing to perform monitoring and alerting on two access points, which could have allowed a Cyber Security Incident to go undetected. Further, failure to track and maintain a list of personnel with cyber access to EACMS could have allowed individuals with cyber access to EACMS to manipulate or alter logical access authorizations to Critical Cyber Assets (CCAs), either purposefully or by mistake, resulting in disruption or loss of control of the energy management system or SERC_URE1's portion of the BPS. However, the firewalls were operational and did not permit unauthorized traffic into the ESP and the front-end device behind the firewalls had locally retained the access logs to the involved remote terminal units. Also, for the third issue, the individuals in question would not have cyber access because automated processes would have removed access within 24 hours.

	L	M
1	Violation Start Date	Violation End Date
5	when the Standard became mandatory and enforceable on SERC_URE1	Mitigation Plan completion
6	seven days past when the accounts were implemented on the device	when the individuals access was revoked and the list was updated

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
5	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Report	To mitigate the first incident in this violation, SERC_URE1: 1) conducted an inventory and developed a list of serial electronic access points; and 2) determined a compliance approach for serial electronic access points and included them in the EACM inventory. To mitigate the second incident in this violation, SERC_URE1: 1) developed a list of all EACM accounts which were opened without proper approvals; 2) obtained account approvals; 3) submitted a survey to peer utilities on best practices for obtaining account approvals; and 4) assessed the survey results to determine if updates were needed to electronic access control and account management procedure. To mitigate the third incident in this violation, SERC_URE1: 1) correctly set security control configuration settings on the replacement asset; 2) decommissioned the asset; and 3) published a policy to ensure continued compliance. To mitigate the fourth incident in this violation, SERC_URE1 removed the user's access and updated the user access review procedures to indicate the need to escalate tickets requesting removal or change of access by following up all ticket requests with a direct email to the user administration personnel responsible for access removal and changes.	8/13/2013	TBD	Neither Admits nor Denies
6	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Report	To mitigate this violation, SERC_URE1: 1) had its networking engineers update the address in the firewall configuration manager and reconfigure the connector; and 2) had its networking management review the connector status and similar issues as part of daily operation meetings by the cyber security operations team. To mitigate this violation, SERC_URE1 will communicate with various groups that are responsible for creating accounts to make them aware of the requirement to notify the personnel that need to update the user account list.	9/30/2014	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
5	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's CIP-005 R1 compliance history to be an aggravating factor in the penalty determination.
6	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
7	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013012994	CIP-004-3	R4	Lower	Lower	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individual had a completed personnel risk assessment, the required cyber security training, and was authorized to have cyber access.
8	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2014013403	CIP-002-1	R3	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The switches were serially connected to devices that converted Ethernet to serial communications and could not be electronically accessed due to the lack of an IP address, which decreased their risk of being compromised and rendered inoperable from an attack. No harm is known to have occurred.
9	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2011007222	CIP-007-1	R6	Lower	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). All of the Cyber Assets, including those involved with this violation, were secured within an established Physical Security Perimeter and ESP. In addition, any external access to the Cyber Assets required strong two-factor authentication.

	L	M
1	Violation Start Date	Violation End Date
7	the eighth day after the individual was granted authorized cyber access to CCAs	when the cyber access list was updated
8	when the Standard became mandatory and enforceable on SERC_URE1	when SERC_URE1 replaced the devices
9	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
7	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Report	To mitigate this violation, SERC_URE1: 1) added the individual at issue to the Cyber Access List; 2) added an item to the employee entrance checklist to ensure a cyber request form is provided to the hiring management if an employee's job function will require cyber access. Hiring management must complete the cyber approval form and provide the form to the cyber access approver. This is done prior to approving physical access; 3) informed affected management of the updated processes; and 4) moved responsibility for performing the quarterly access review from plant operations into the generation compliance group. The physical access approver provides the required physical documents. The cyber access approver, physical access approver, and the generation compliance representative perform the quarterly review together.	9/17/2013	8/6/2014	Neither Admits nor Denies
8	$29,000 (for SERC2013011812, SERC2013012154, SERC2013012155, SERC2013012520, SERC2013012994, and SERC2014013403)	Self-Report	To mitigate this violation, SERC_URE1: 1) installed layer two devices which do not allow for IP configuration, identifying the devices as non-critical cyber systems; and 2) reviewed the CCA Classification procedure and conducted a training session on the proper identification of CCAs and non-CCAs.	2/4/2014	4/4/2014	Neither Admits nor Denies
9	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Self-Report and Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) for the first issue: a) removed the affected Cyber Assets' ability to use a routable protocol within a control center by disconnecting the network cable. In addition, the Cyber Assets were tagged with a warning stating "do not connect to any network." This action prevents any possible misuse of the Cyber Assets; b) updated the CCA list to reflect the removal of the fiber channel switches; c) added a hardware lock to each network port on each of the fiber channel switches to prevent installation of network cables; d) improved applicable internal policies and procedures for adding new Cyber Assets to the ESP. The updates included more diligent analysis of requirements and guidelines for submitting technical feasibility exceptions (TFEs); e) evaluated and selected replacement Cyber Assets that are supported by the chosen vendor and comply with all required NERC CIP Standards; f) requested funding for the selected replacement Cyber Assets during next budget cycle; g) purchased replacement Cyber Assets once approved for the budget; h) communicated to and trained personnel, responsible for adding Cyber Assets to the ESP, on the updated policies and procedures; i) tested the acquired replacement Cyber Assets; j) ensured Cyber Assets were compliant with all applicable NERC CIP Standards; k) installed the replacement Cyber Assets into the ESP; and 2) for the second issue: a) completed inventory of applicable Cyber Assets and validated logging was functional; b) filed TFEs as necessary; c) completed a review of current process and controls for remaining Critical Assets to identify gaps; d) updated processes and controls as necessary to close gaps identified; and e) trained personnel on updated processes and controls.	10/17/2012	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
7	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's CIP-004 R4 compliance history to be an aggravating factor in the penalty determination.
8	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's CIP-002 R3 compliance history to be an aggravating factor in the penalty determination.
9	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
10	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2011007238	CIP-004-3	R4	Lower	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All of the individuals involved possessed a valid personnel risk assessment and had the required cyber security training.
11	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009709	CIP-002-1	R1	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failure to consider required asset types when developing the RBAM could have resulted in Critical Assets not being correctly identified and afforded protective measures required by the CIP Standards. The proper identification of Critical Assets is crucial to the reliable operation of the BPS. Without this, Critical Cyber Assets (CCAs) upon which the Critical Assets rely for functionality are not afforded all of the protective measures of the CIP Standards. Without these protective measures, the CCAs were at a greater risk of being compromised and rendered inoperable, whic increases the risk to Critical Assets becoming compromised and/or rendered inoperable. However, SERC_URE2's agent had developed an RBAM for its registered functions that considered the required asset types and had identified the CCAs used in the course of performing SERC_URE2's registered functions. The CCAs were protected pursuant to the SERC_URE2 agent's CIP program.
12	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009712	CIP-003-1	R2	Medium	Lower	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2's failure to document the designation of a senior manager could have resulted in unauthorized personnel approving CIP documents. However, there was an employee acting as the senior manager.

	L	M
1	Violation Start Date	Violation End Date
10	when SERC_URE2's agent failed to remove the individual from the access lists	when SERC_URE2's agent added users to the access lists
11	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion
12	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
10	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Self-Report and Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) for the first issue: a) revoked CCA access; b) verified employees' CCA access; c) verified other business units' employees' CCA access; d) conducted a review of all current processes, procedures, and training in support of CIP-004 R4 to identify improvements reducing the probability of reoccurrence; e) revised CIP-004 processes as needed; f) investigated and implemented a local solution that incorporated automatic notification escalation of pending revocation requests; and g) trained impacted supervisors on updated processes; and 2) for the second issue: a) validated its access list used to track personnel to ensure that the list was consistent with existing access authorization and/or revocation documentation and its other departments conducted an extent of condition analysis to validate their respective access lists were consistent with existing access authorization and/or revocation documentation; b) performed a review of its current processes for maintenance of its access lists and, as necessary, identified process improvements focused on automating the generation of the access list and enhancing the existing technical and procedural controls for the maintenance of the access lists; c) revised processes and procedures for each department where improvements were identified; and d) trained affected employees on the revised processes and procedures.	10/31/2012	TBD	Neither Admits nor Denies
11	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2: 1) revised its RBAM document used to identify its Critical Assets to include all of the asset categories required by R1.2.	11/10/2011	TBD	Neither Admits nor Denies
12	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2: 1) created a new change in senior manager assignment document.	11/10/2011	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
10	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's CIP-004 R4 compliance history to be an aggravating factor in the penalty determination.
11	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.
12	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
13	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009713	CIP-005-1	R1; R1.5	Medium	Severe	The violation posed a moderate risk to the reliability of the bulk power system. Failing to identify and to protect electronic access control and monitoring devices could introduce vulnerabilities to the ESP and subsequently, the Critical Cyber Assets located therein. However, the device had been afforded the other protective measures listed in CIP-005-1 R1.5.
14	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009714	CIP-005-1	R3; R3.2	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to monitor access to the ESP may result in unauthorized access going undetected. However, the firewalls were configured to log denied traffic, which provided the ability to alert to unsuccessful unauthorized access attempts. In addition, interactive access into the ESP required strong two-factor authentication.

	L	M
1	Violation Start Date	Violation End Date
13	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion
14	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
13	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) performed an assessment and extent of condition review of asset type classification for Cyber Assets in scope of CIP-005 R1.5; 2) performed a cyber vulnerability assessment (CVA) per CIP-007 R8 for the Cyber Asset identified in the Compliance Audit as being improperly classified and, thus, did not have a CVA completed. Additionally, performed an extent of condition review of CIP-007 R8 and sub-requirements for all applicable Cyber Assets used in the access control and/or monitoring of the ESPs; 3) performed training and education on the applicability of standards and requirements associated with Cyber Assets used in the access control and/or monitoring of the ESPs as per CIP-005 R1.5; and 4) implement corrective actions as identified in action plans created in the milestones for applicable Cyber Assets used in the access control and/or monitoring of the ESPs across business units.	7/11/2013	TBD	Neither Admits nor Denies
14	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) researched how to technically implement a mechanism to detect and alert for actual unauthorized accesses or determine if a procedural process can be implemented should a technical solution not be available; 2) submitted a Technical Feasibility Exception (TFE) for Cyber Assets that could not detect and alert for actual unauthorized accesses. In addition, SERC_URE2's agent's remaining departments that operate the rest of its Critical Assets conducted an extent of condition analysis on their Cyber Assets and confirmed that those assets could detect and alert for actual unauthorized accesses; 3) created procedures to detect and alert for actual unauthorized accesses for any Cyber Assets on which it is not technically feasible to do so. In addition, SERC_URE2's agent's remaining departments that operate the rest of its Critical Assets will submit a TFE for Cyber Assets that cannot detect and alert for actual unauthorized accesses identified in the previous milestone as needed; 4) performed a review of build/test plans for Cyber Assets subject to CIP-005 R3 to ensure that they included steps for validating that the Cyber Assets are configured to detect and alert for attempts at or actual unauthorized accesses 24 hours a day, seven days a week. Additionally, language will be enhanced to ensure that when automated alerting is not technically feasible, a TFE will be filed and the Cyber Assets will be subject to processes and procedures created in the previous milestone to assess access logs for attempts at or actual unauthorized accesses at least every 90 calendar days; 5) trained all personnel responsible for performing the new procedures created in the previous milestone as needed; and 6) implemented any new processes created in the previous milestone.	6/27/2013	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
13	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.
14	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
15	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009715	CIP-006-1	R1; R1.8	Medium	Severe	The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failing to protect Physical Access Control System (PACS) devices could result in unauthorized individua gaining access to Critical Cyber Assets, which could impact the BPS. However, the affected Cyber Assets were secured within a PSP with access control and monitoring and required two-factor authentication to access.
16	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009716	CIP-007-1	R2; R2.2	Medium	Severe	The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failing to disable ports and services that are not required for emergency or normal operations could allow unauthorized users to gain access and control of Cyber Assets or provide an opportunity for malware to be introduced. However, the devices resided in an Electric Security Perimeter and a Physical Security Perimeter, In addition, any external access to the Cyber Assets required strong two-factor authentication.

	L	M
1	Violation Start Date	Violation End Date
15	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion
16	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
15	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) collaborated with manufacturer via email and phone to confirm the operator table and password history table should be in sync and that SERC_URE2's agent's results could be replicated in the manufacturer's lab to ensure it was not specific to the SERC_URE2 agent's environment; 2) created a script that will automatically notify users via email if their password has not been changed in 305 days (60 days before 365 days limit), 335 days (30 days before 365 days limit) and 358 days (7 days before the 365 days limit); 3) created a script that will automatically notify via email the access control intrusion detection system application administrators if any account password has not been changed in 359 days or more and request the administrator to terminate and/or disable the account; 4) updated corporate security document to reflect the notifications outlined in previous two milestones. The on-call administrator will delete the account and record in a service ticket upon receipt of the notification of account passwords exceeding 359 days; 5) trained corporate security personnel responsible for the updates made to corporate security systems security management document; 6) communicated to users in the access control intrusion detection system the requirement to change their password annually and failure to change their password annually would result in their account being terminated before their annual date; 7) conducted an extent of condition analysis of the PACS devices in regards to the protective measures in CIP-007-3 and determined if there are any gaps that needed to be addressed with the outlined protective measures; 8) reviewed the results of the extent of condition analysis in the previous milestones to develop a corrective action plan to address any identified gaps; 9) completed the corrective action plan developed in previous milestone; 10) communicated to and trained affected personnel on the changes from the corrective action plans completed in the previous milestone; 11) information management performed an extent of condition review for the PACS servers in relation to CIP-007 R3 controls, and established a corrective action plan to address any issues or improvements identified during the reviews; and 12) performed an extent of condition review of account management controls for the PACS servers in regards to CIP-007 R5 (including need to file additional TFEs), and established a corrective action plan to address any issues or improvements identified during the reviews. SERC_URE2's agent implemented corrective actions as identified in action plans created in previous two milestones for PACS Cyber Assets across business units.	7/11/2013	TBD	Neither Admits nor Denies
16	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) ascertained required ports and services for normal and emergency operations; 2) determined if any updates to procedures were needed; 3) updated process documents as needed from prior milestone; 4) trained personnel; 5) reviewed current CIP assets and validated required ports for normal and emergency operations of the asset were correctly documented; and 6) reviewed current CIP assets and validated that the cyber vulnerability assessments performed were adequate and update any discrepancies identified.	3/31/2013	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
15	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC determined that SERC_URE2's compliance history should not serve as a basis for aggravating the penalty.
16	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC determined that SERC_URE2's compliance history should not serve as a basis for aggravating the penalty.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
17	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009717	CIP-007-1	R4	Medium	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Cyber Assets involved were power distribution devices for servers at a manned site and could be bypassed immediately to maintain operations if they had become compromised. In addition, the Cyber Assets resided behind firewalls with access controls that restricted unauthorized traffic and resided within Physical Security Perimeter.
18	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009718	CIP-007-1	R3	Lower	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Cyber Assets resided within a Physical Security Perimeter and ESP, and all personnel with access had valid Personnel Risk Assessments and current cyber security training.
19	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009719	CIP-007-1	R5; R5.3	Medium	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Cyber Assets resided in an ESP and a Physical Security Perimeter. Any external access to the Cyber Assets required strong two-factor authentication. For the Cyber Assets that could not enforce password complexity, passwords were still in place. For those passwords that were not changed annually, the accounts were locked by the system as they were not accessed within the required timeframe.

	L	M
1	Violation Start Date	Violation End Date
17	when the Standard became mandatory and enforceable on SERC_URE2	when SERC_URE2's agent submitted a TFE
18	when the Standard became mandatory and enforceable on SERC_URE2	when SERC_URE2's agent implemented the patch management program for the affected Cyber Assets
19	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
17	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) submitted appropriate TFEs; 2) performed an inventory of Cyber Assets related to the affected location; 3) completed TFEs for any Cyber Assets identified as needed; 4) reviewed current process and identified any potential gaps in evaluating the need for a TFE; and 5) updated policies and procedures, and trained personnel.	1/29/2013	TBD	Neither Admits nor Denies
18	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) performed a review of current patch management procedures; 2) conducted an analysis of all applicable Cyber Assets and categorized applicable security patches; 3) performed an analysis to determine what operating system, software, applications, and firmware were not currently included in the procedure(s) fo formal tracking; 4) updated associated patch management procedures for any identified gaps; 5) updated and released new versions of all applicable patch management programs; and 6) conducted training.	11/30/2012	TBD	Neither Admits nor Denies
19	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) completed the TFE documentation and submitted the TFEs; 2) performed a review of account(s) for CIP assets and ensured that passwords have been changed within the annual requirement; 3) reviewed remaining accounts for annual password changes and changed any passwords that needed to be changed; 4) completed a review of current processes and controls to identify gaps; 5) completed and submitted TFEs for any assets identified in previous milestones as needed; and 6) updated the processes and controls as identified, and completed training of personnel.	1/15/2013	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
17	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.
18	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.
19	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
20	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009721	CIP-007-1	R8; R8.2	Lower	Severe	The violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to review ports and services during the annual CVA could allow unnecessary ports and services to remain open and vulnerable to exploit. However, logging was properly configured, which alerted to security events. In addition, all of the involved Cyber Assets were within an ESP and a Physical Security Perimeter.
21	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2012009722	CIP-006-3a	R1; R1.7	Lower	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2's agent updated the physical security plan within 70 days of the change and the site security system was functioning properly.

	L	M
1	Violation Start Date	Violation End Date
20	when SERC_URE2's agent had to complete the annual CVA properly	Mitigation Plan completion
21	30 days after SERC_URE2's agent should have updated the physical security plan	when SERC_URE2's agent updated the physical security plan

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
20	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) ascertained required ports for normal and emergency operations of the assets; 2) reviewed processes and procedures related to required ports and services; 3) updated procedures based on results of prior milestone; 4) trained personnel; 5) performed review of current CIP assets and validated required ports for normal and emergency operations are correctly documented; and 6) performed a review of current CIP assets and validated CVAs were adequate and updated discrepancies identified.	3/31/2013	TBD	Neither Admits nor Denies
21	$0 (for SERC2011007222, SERC2011007238, SERC2012009709, SERC2012009712, SERC2012009713, SERC2012009714, SERC2012009715, SERC2012009716, SERC2012009717, SERC2012009718, SERC2012009719, SERC2012009721, and SERC2012009722)	Compliance Audit	To mitigate this violation, SERC_URE2's agent: 1) conducted an extent of condition analysis of physical security perimeters at designated Critical Assets to determine whether there were other instances in which the physical security plan was not updated within 30 days following a reconfiguration or redesign change; 2) reviewed results of extent of condition analysis. If additional instances were identified in which the physical security plan was not updated following a reconfiguration or redesign change, added all necessary updates to the next revision of the physical security plan; 3) collected all applicable physical security drawings related to physical security perimeters for designated Critical Assets from each of the respective business areas; notified business areas that corporate security would assume custodianship and retention responsibilities of the physical security drawings going forward to include within the updated physical security plan; 4) updated physical security plan to include language stating that the physical security plan will be updated and signed by the director of corporate security, as the Senior Manager delegate for CIP-006, to incorporate any physical security redesign or reconfiguration changes (including, but not limited to, additional or removal of access points through the physical security perimeter, physical access controls or monitoring/logging controls) within 30 days. The updates to the physical security plan also specified that it is corporate security's responsibility to be the custodian of all applicable the physical security drawings related to physical security perimeters for designated Critical Assets which will be included within the physical security plan; 5) updated corporate security's workflow documentation for CIP-006 R1.7 to include a notification to the director of corporate security, as a checkpoint when a physical security configuration change ticket is closed out for any physical security reconfiguration or redesign of physical security perimeters at designated Critical Assets; 6) communicated to corporate security personnel the updated workflow for CIP-006 R1.7; and 7) communicated and conducted training to the applicable business areas regarding the changes to the enterprise physical security plan implemented.	4/27/2012	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
20	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC considered SERC_URE2's compliance history and determined there were no relevant instances of noncompliance.
21	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition, SERC_URE2 and SERC_URE2's agent completed the following actions, which SERC considered to be a mitigating factor in the penalty determination. SERC_URE2 revised its RBAM, Critical Asset list, and CCA list to clearly indicate that SERC_URE2's agent's RBAM, Critical Asset list, and CCA list identify the relevant Cyber Assets necessary to support SERC_URE2's registered functions. In addition, SERC_URE2's agent provided SERC with documentation that clearly identifies all Critical Assets, CCAs, Electronic Access Control or Monitoring Systems, and Physical Access Control Systems involved in supporting SERC_URE2's registered functions. These updated documents will enable SERC to more quickly identify any CIP issues that involve SERC_URE2's registered functions and minimize the impact on SERC_URE2's agent if future possible violations are discovered. SERC determined that SERC_URE2's compliance history should not serve as a basis for aggravating the penalty.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
22	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2013012824	CIP-004-3	R4; R4.1	Lower	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All three instances were documentation errors and all individuals' physical access were removed despite the failure to update the access list. Additionally, all individuals involved had cyber security training, had a completed personnel risk assessments, were in good standing, and had not been terminated for cause.
23	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2013012825	CIP-007-3a	R1	Medium	Severe	This violation posed a minimal risk, and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk of the violation was reduced by the following factors. The generic account was discovered on the same day it was re-enabled as a result of the power interruption. The generic account was disabled four days later with the configuration saved to permanent memory, ensuring the issue would not recur. SERC_URE3 tested its cyber security controls when it first deployed the network switch and found no adverse effects. The switch was located within a protected Physical Security Perimeter and ESP. Additionally, there were other protective measures in place such as network segmentation, isolation of security zones, firewalls, intrusion detection and prevention systems, and 24 hours a day, seven day week monitoring provided by a security services provider. There were no Cyber Security Incidents reported during the violation.

	L	M
1	Violation Start Date	Violation End Date
22	when the first individual was added to the access list in error	when the last individual was removed from the access list
23	when the network switch was deployed	when the configuration was appropriately saved

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
22	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) conducted a line-by-line review of the printed reports from the source system and the access list; 2) remedied all identified discrepancies in the existing CCA access lists; 3) conducted periodic line-by-line reviews of the printed source reports from the source system and the access list; 4) held a formal training session that included all employees responsible for using the access/install/moves (AIM) tool to grant and remove physical access; 5) circulated an email to affected personnel describing a more detailed AIM report to use for adding and removing access and the importance of following this process; and 6) fully implemented an automated program that checks for discrepancies between the source system and the access list every evening.	10/18/2013	TBD	Neither Admits nor Denies
23	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) removed the unapproved generic account from the network switch; 2) added a step to the checklist to prompt the saving of the configuration to an extensively detailed, step-by-step checklist for preparation and deployment of every CIP Cyber Asset; and 3) circulated an email to affected personnel describing the new work instruction that was added to the checklist and the importance of saving the configuration.	6/6/2014	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
22	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.
23	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
24	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2013012826	CIP-007-3a	R6	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). This violation affected a single generation facility which was not in operation during the violation. Therefore, the six Cyber Assets involved were not functionally utilized during the violation. There were no reportable Cyber Security Incidents during the violation. Further, the Cyber Assets were within a protected ESP and Physical Security Perimeter. Additionally, there were other protective measures in place such as network segmentation, isolation of security zones, firewalls, intrusion detection and prevention systems, and 24 hour a day, seven day week monitoring provided by a security services provider.
25	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2013012941	CIP-005-3a	R1; R1.5	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). A lack of processes, procedures, and proper tools to identify and document electronic access points greatly increased the risk of Critical Cyber Assets (CCAs) being compromised and rendered inoperable. In addition, failing to identify and protect EACM devices could introduce vulnerabilities to the ESP and subsequently, the CCAs located therein. However, for the first instance, electronic access was restricted to 13 network engineers that had a completed personnel risk assessment and cyber security training. For the second instance, procedures were in place and staff was trained and prepared to perform the disaster recovery plan test for the two EACM devices. Further, SERC_URE3 performed a disaster recovery plan test for other Cyber Assets within the ESP. For the third instance, the failure to test in the test environment was identified and mitigated the following day. Also, although the service pack was not tested prior to implementation, the subsequent testing of the service pack confirmed that the content of the updates wa not critical to the management system. No identified cyber incidents occurred during the duration of the violation. All devices involved in this violation were protected within a secure Physical Security Perimeter and ESP. Further, the devices in question could only be electronically accessed by individuals with two-factor authentication and SERC_URE3 has signature and behavioral based intrusion detection system devices in place to alert personnel in the event of suspicious activity.

	L	M
1	Violation Start Date	Violation End Date
24	when the firewall configuration was changed and logging and monitoring stopped for the six devices	when the firewall configuration was modified to ensure logging resumed
25	when the firewall began acting as an access point	present

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
24	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) corrected the ruleset to allow alerting; and 2) created alarms to notify support personnel of potential loss of logging.	11/17/2013	TBD	Neither Admits nor Denies
25	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) modified site-to-site VPN tunnels peering with existing ESP access points to not allow interface access control lists on ESP access points to be bypassed; 2) updated the checklist for adding or replacing CIP assets to specify that new access point firewalls using VPN tunnels should not be configured in a manner that allows VPN sessions to bypass interface access control lists; 3) completed the CIP-009 R2 annual recovery exercise for the two EACM systems not previously included; 4) updated the checklist for adding or replacing CIP Assets to specify that the annual recovery plan exercise and backup media testing must be performed in the initial year; 5) tested the service pack after-the-fact to determine that it had no adverse effects to the cyber security controls; 6) made technical enhancements to servers to ensure that administrators could easily distinguish between test and production server console sessions; 7) made enhancements to the managed security service provider (MSSP) internal procedures used in applying security patches to the servers; 8) the MSSP completed training of all engineers that have access to the SERC_URE3 network; 9) performed scoping of all CIP environments to ensure no other instances of access point firewalls using VPN tunnels configured in a manner that allows VPN sessions to bypass interface access control lists exists; 10) developed technical enhancement to automatically audit configurations to ensure there is no bypass checkbox checked; and 11) developed and provided training on access point and site-to-site VPN tunnel configuration. To mitigate this violation, SERC_URE3 will uncheck the bypass checkbox in all CIP environments.	2/10/2015 (approved completion date)	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
24	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.
25	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
26	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2013012942	CIP-005-3a	R2; R2.1; R2.4; R2.5	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failing to establish processes and mechanisms that use an access control model that denies access by default gave approximately 1,305 users unauthorized access to the energy management system (EMS) network, increasing the risk of Critical Cyber Assets (CCAs) being accessed, compromised, and rendered inoperable. In addition, failing to implement and to document organizational processes and strong technical and procedural mechanisms to ensure the authenticity of users accessing the ESPs could have resulted in unauthorized individuals gaining access to the ESP and CCAs therein. However, access to the EACM (firewall) configurations (ACLs) was restricted to authorized personnel only and was based on job function. In all three instances, SERC_URE3 reviewed log files to confirm that no suspicious activity occurred. A managed security services provider was monitoring for detected security events throughout the network 24 hours per day, 7 days per week. No Cyber Security Incidents were reported during this violation. SERC_URE3 had protective controls in place on CCAs and Cyber Assets inside of established ESPs and two-factor authentication was required for all remote access to SERC_URE3 systems. In instance one, most of the users were unaware of their ability to access the EMS network. The three employees that accessed the EACM server were network administrators and had access to network devices but did not have local access to devices inside of the network. Accessing CCAs within the ESPs would require user accounts and passwords for the relevant CCAs. The three employees were authorized for electronic access to CCAs, had valid personnel risk assessments, and had undergone cyber security training. SERC_URE3 reviewed logs and confirmed that the three individuals did not attempt to access any CCAs via the EACM server during the violation. Also, two-factor authentication was required to access the VPN, making it difficult for a malicious individual to take advantage of the misconfigured ACL associated with the VPN group policy. For instances two and three, no employees used the access that they had been granted.

	L	M
1	Violation Start Date	Violation End Date
26	when an EACM device was installed without a deny-by-default configuration	when the electronic access list in instance one was modified

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
26	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) modified the VPN group policy to include an ACL with a default deny rule; 2) removed the CIP subnet from the ACL; 3) corrected the access discrepancies for the three individuals mentioned in the self-report; 4) created a separate business to business (B2B) VPN remote access server specifically for use with CIP Assets and migrate to that server the remote access function for EACM systems; 5) created a separate B2B VPN remote access server specifically for use with CIP Assets and migrated to that server the remote access function for ESPs and Physical Access Control Systems; 6) created alerts that trigger when specific changes are made in the configuration of network equipment, specifically switches, routers, and firewalls; and 7) developed and provided training on the processes and requirements specific to granting and removing external interactive access into ESPs. To mitigate this violation, SERC_URE3 will enhance existing technical controls to further delineate the type and level of access privileges for administrative access to network equipment (specifically switches, routers, and firewalls) and will enhance the granularity of role based authentication and authorization policies for network administrators.	2/10/2015 (approved completion date)	TBD	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
26	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
27	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2014013882	CIP-004-3a	R4; R4.1; R4.2	Lower	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individuals involved had cyber security training and completed personnel risk assessments. For the first issue, the individual involved was authorized for the access that was granted. The error in the access list was corrected two days after discovery. Also, this issue affected 0.04% of those who were listed accurately on the access list. Finally, the domain that the user was granted access to had electronic monitoring. For the second issue, the individual involved resigned in good standing and the physical access logs for the PSP revealed that the vendor employee's card was not used to access the PSP during the violation. For the second and third issue, the PSP in question was manned 24 hours a day, 7 days a week by SERC_URE3 personnel. This PSP contains no CCAs, only EACMs and non-CCAs. For the third issue, SERC_URE3 was in possession of the access card since its creation. The vendor employee had not visited the SERC_URE3 site and never had possession of the access card. Therefore, the vendor employee had no means to access the PSP, which contained EACM devices but no CCAs.
28	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013011963	CIP-005-3	R2	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this case, WECC_URE1 failed to ensure that only ports and services required for operations and monitoring of Cyber Assets within the ESP were enabled on three firewalls. This violation posed potential harm to WECC_URE1, because additional points of vulnerability to the ESP could be created, due to WECC_URE1's failure to disable ports and services. However, the risk posed by WECC_URE1's failure is limited given compensating measures in place during the violation period. WECC_URE1 has a "defense-in depth" cybersecurity strategy. Each of the three devices was configured to deny access by default, such that explicit access permissions must be specified. Electronic access to the devices was limited to individuals who required such access to perform their job function. Access through each ESP access point was monitored and logged 24-hours a day, seven days a week. Unauthorized access attempts would have triggered an alarm that alerted designated personnel.
29	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013011964	CIP-005-3a	R4	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This violation posed potential harm to WECC_URE1, because WECC_URE's failure to conduct timely CVAs could affect the stability and availability of WECC_URE1's immediate operational area of coverage. The risk posed by WECC_URE1's noncompliance is, however, offset given compensating measures in place during the violation perio WECC_URE1 implemented a defense-in-depth architecture of administrative, physical and logical cyber security controls. Electronic access through each firewall was limited to individuals who completed Personnel Risk Assessments and cybersecurity training. The four ESP access points were configured to deny access by default, such that explicit access permissions must be specified. Electronic access to the devices was limited to individuals who required such access to perform their job function. Access through each ESP access point was monitored and logged 24-hours a day, seven days a week. Unauthorized access attempts would have triggered an alarm that alerted designated personnel.
30	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013011875	CIP-006-1	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE1 failed to ensure that only ports and services required for normal and emergency operations were enabled on 19 devices used in the access control and monitoring of the PSP. This violation posed potential harm to WECC_URE1 because the access control and monitoring devices to its PSP could have been vulnerable to misuse of malicous cyber attacks. The potential risks associated with this violation were however, limited due to WECC_URE1's additional procedures and policies. Specifically, WECC_URE1 had limited communication through the firewall to on necessary communication. Additionally, the PACS ESP does not contain any Critical Cyber Assets (CCAs) and is not connected to a CCA ESP. Individuals with electronic access to the ESP completed Personnel Risk Assessments and cyber security training.

	L	M
1	Violation Start Date	Violation End Date
27	eight days after the first individual was granted access	Mitigation Plan completion
28	when the Standard became mandatory and enforceable on WECC_URE1 as a "Table 1" entity	Mitigation Plan completion
29	when WECC_URE1 failed to conduct an annual review	The last day of the noncompliant CVA year
30	when the Standard became mandatory and enforceable on WECC_URE1 as a "Table 1" entity	Mitigation Plan completion

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
27	$30,000 (for SERC2013012824, SERC2013012825, SERC2013012826, SERC2013012941, SERC2013012942, and SERC2014013882)	Self-Report	To mitigate this violation, SERC_URE3: 1) remedied the identified discrepancy in the existing access list; 2) implemented a technical enhancement to identify a discrepancy between the two tables in the future and thus prevent a potential violation in the future; 3) removed physical CIP Access for the vendor employee in the second issue; 4) removed physical CIP Access for all vendor employees in the second issue; 5) removed physical CIP Access for the vendor employee in the third issue; and 6) removed physical CIP Access for all parent company employees and parent company vendor employees.	7/29/2014	TBD	Neither Admits nor Denies
28	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) disabled the non-required ports and services; and 2) created a checklist to be used when any future significant changes occur.	3/20/2013	6/14/2013	Agrees
29	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) updated its CVA processes to include additional reviews; 2) created a correction statement to address the error in the 2011 report; and 3) reviewed the 2011 and 2012 CVAs for potential issues using the new review process.	6/21/2013	10/18/2013	Agrees
30	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Self-Report	To mitigate this violation, WECC_URE1: 1) addressed PACS servers' known ports and services to complete CIP controls implementation; 2) addressed deficiencies; and 3) updated its Cyber Asset Security Checklists for each device with final status to validate CIP Controls Implementation.	3/13/2014	3/22/2014	Agrees

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
27	SERC reviewed SERC_URE3's Internal Compliance Program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history to be an aggravating factor in the penalty determination.
28	WECC reviewed WECC_URE 3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
29	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
30	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

	A	B	C	D	G	H	I	J	K
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
31	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012011493	CIP-007-1	R2	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE1 failed to ensure that ports and services required for normal and emergency operations were enabled on seven devices located within its EMS ESP. This violation posed potential harm to WECC_URE1 because its non-compliance created opportunities for unauthorized internal cyber attacks. The potential risks associated with this alleged violation were, however, limited due to WECC_URE1's additional procedures and policies. Specifically, the EMS network devices have technical and procedural controls for electronic access at all access points. Additionally, passwords are required to access the devices and all EMS devices are located within a Physical Security Perimeter PSP which is monitored 24 hours a day, 7 days a week.
32	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012011494	CIP-007-1	R3	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this case, WECC_URE1 failed to assess patches for legacy applications installed on 27 EMS devices and three PACS devices. This violation posed potential harm to WECC_URE1 because its noncompliance created opportunities for unathorized internal cyber attacks. However, the devices in scope of the violation did not have internet connectivity. In the event that software vulnerabilities existed, they could not be accessed nor exploited externally from the internet. Further, legacy programs were not running during the violation period and could not be accessed internally, limiting the risk during the violation. The risk of internal misuse was offset given compensating measures in place during the violation period. Internal electronic access to the devices was limited to individuals who completed Personnel Risk Assessments and cybersecurity training. The devices were physically secured within Physical Security Perimeters PSP and ESP Electronic Security Perimeters. All access was logged and monitored. Unauthorized physical or electronic access attempts would have triggered an alarm, alerting appropriate WECC_URE1 personnel.
33	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013012008	CIP-007-3a	R5	Lower	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This violation posed potential harm to WECC_URE1, because if unauthorized access to the Cyber Assets is not logged, and is unnoticed and unchecked, it could allow potentially malicious access to these assets. The risk posed by WECC_URE1's noncompliance is limited given the compensating measures in place during the violation period. Each of the 12 devices were located within an Electronic Security Perimeter (ESP). Although access logs for the individual CCAs were not maintained for 90 days, access logs for the ESP were generated, maintained and reviewed during the violation period. Unauthorized access through the ESP would have been detected through WECC_URE1's use of alarms. Unauthorized access attempts would have triggered an alarm alerting WECC_URE1 information technology staff. Additionally, electronic access to the ESP and CCAs in scope of the violation was restricted to individuals who completed Personnel Risk Assessments and cybersecurity training.
34	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013727	CIP-005-3a	R1; R1.5	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE2 failed to provide evidence of annual testing of backup media for Cyber Assets used in the access control and/or monitoring of the ESP. However, WECC_URE2 implemented alternative procedures to help detect corrupt backup disks and to help prevent the use of outdated information for restoration. Specifically, WECC_URE2 implemented an enterprise media backup and management system for the testing of backup disks. While this system only conducts tests on samples of Cyber Asset systems, the testing is done monthly which aids in the detection of corrupt data. Further, WECC_URE2 ensured that every CCA resided within an Electronic Security Perimeter (ESP) and that WECC_URE2 identified and documented the ESPs and all access points to the perimeter. WECC_URE2 performs monthly testing of all backup media types in addition to annual sample testing.
35	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2014013752	CIP-005-3a	R1; R1.5	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 failed to provide evidence of annual testing of backup media for Cyber Assets used in the access control and/or monitoring of the ESP. However, WECC_URE3 implemented alternative procedures to help detect corrupt backup disks and to help prevent the use of outdated information for restoration. Specifically, WECC_URE3 implemented an enterprise media backup and management system for the testing of backup disks. While this system only conducts tests on samples of Cyber Asset systems, the testing is done monthly which aids in the detection of corrupt data. Further, WECC_URE3 ensured that every CCA resided within an Electronic Security Perimeter (ESP) and that WECC_URE3 identified and documented the ESPs and all access points to the perimeter. WECC_URE3 performs monthly testing of all backup media types in addition to annual sample testing.

	L	M
1	Violation Start Date	Violation End Date
31	when the Standard became mandatory and enforceable on WECC_URE1 as a "Table 1" entity	Mitigation Plan completion
32	the day after WECC_URE1 completed the mitigation of its first violation of the Standard	Mitigation Plan completion
33	the day after WECC_URE1 completed the mitigation of its first violation of the Standard	Mitigation Plan completion
34	the first day of the calendar year in which WECC_URE2 cannot demonstrate compliance with the Standard	when WECC_URE2 had evidence of testing of backup media for EACM devices
35	the first day of the calendar year in which WECC_URE3 cannot demonstrate compliance with the Standard	when WECC_URE3 had evidence of testing of backup media for EACM devices

	N	O	P	Q	R	S
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"
31	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Self-Report	To mitigate this violation, WECC_URE1: 1) identified, validated, and documented authorization of ports and services for PACS and EMS devices; 2) listed authorized ports and services, including dynamic ranges; 3) create a new testing checklist for changes to applicable Cyber Assets; and 4) train WECC_URE1's subject matter experts on the new procedures.	10/31/2013	2/18/2014	Agrees
32	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Self-Report	To mitigate this violation, WECC_URE1: 1) scoped and mitigated PACS systems, network devices, and EMS systems; 2) updated patch program to include application patch requirements; and 3) verified that there were no more unknown patches that require assessing and scheduling of patch deployment.	9/5/2014	9/18/2014	Agrees
33	$65,000 (for WECC2013011963, WECC2013011964, WECC2013011875, WECC2012011493, WECC2012011494, and WECC2013012008)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) fixed its logging procedures to server for user authentication; 2) reviewed logs from the devices; 3) removed one device,; and 4) created a Cyber Asset Security Checklist.	5/20/2013	9/27/2013	Agrees
34	$0	Compliance Audit	To mitigate this violation, WECC_URE2: 1) modified the procedure for annual testing of backup media to specifically include EACMs as an asset type; and 2) enhanced the process for conducting monthly verification of backup media images in a manner that results in appropriate evidence retention and comprehensive coverage of all applicable Cyber Assets.	6/13/2014	9/22/2014	Neither Admits nor Denies
35	$0	Compliance Audit	To mitigate this violation, WECC_URE3: 1) modified the procedure for annual testing of backup media to specifically include EACMs as an asset type; and 2) enhanced the process for conducting monthly verification of backup media images in a manner that results in appropriate evidence retention and comprehensive coverage of all applicable Cyber Assets.	6/13/2014	9/22/2014	Neither Admits nor Denies

	T
1	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
31	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
32	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
33	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
34	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC also considered two other mitigating factors. First, WECC_URE2 provided an affidavit to WECC stating that it was actually performing monthly testing of backup images for all asset types, but that WECC_URE2 failed to create and maintain evidence of such testing. Second, WECC_URE2 underwent a prior Compliance Audit. During that audit, WECC_URE2's procedure for annual testing of backup media was in effect, but WECC did not find deficiencies with WECC_URE2's backup media testing program, thereby perpetuating WECC_URE2's determinations with respect to the satisfactory nature of its compliance documents regarding testing of backup media, resulting in the current violation.
35	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC also considered two other mitigating factors. First, WECC_URE3 provided an affidavit to WECC stating that it was actually performing monthly testing of backup images for all asset types, but that WECC_URE3 failed to create and maintain evidence of such testing. Second, WECC_URE3 underwent a prior audit. During that Compliance Audit, WECC_URE3's procedure for annual testing of backup media was in effect, but WECC did not find deficiencies with WECC_URE3's backup media testing program, thereby perpetuating WECC_URE3's determinations with respect to the satisfactory nature of its compliance documents regarding testing of backup media, resulting in the current violation.

February 26, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventy thousand dollars ($70,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement and disposition documents. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SERC2013012689	CIP-002-1	R3	High/ Severe	$70,000
SERC2013012691	CIP-005-1	R1; R1.1; R1.5	Medium/ Severe	
SERC2014013574	CIP-005-1	R1; R1.4	Medium/ Severe	
SERC2013011676	CIP-005-1	R3	Medium/ Severe	
SERC2013011702	CIP-006-3c	R1; R1.1; R1.6	Medium/ Severe	
SERC2013012693	CIP-006-1	R3	Medium/ Severe	
SERC2013012695	CIP-007-1	R1	Medium/ Severe	
SERC2013012694	CIP-007-1	R2: R2.1	Medium/ Severe	
SERC2012009565	CIP-007-1	R3	Lower/ Severe	
SERC2012009647	CIP-007-1	R4	Medium/ Severe	
SERC2012009566	CIP-007-1	R5; R5.2; R5.3	Medium/ Severe	
SERC2012009564	CIP-007-1	R6	Medium/ Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-1 R3 (SERC2013012689)

During a Compliance Audit, SERC determined that URE failed to develop a complete list of Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset. Specifically, URE failed to identify network switches as CCAs. URE used the switches between their modem banks and the terminal servers within its Energy Management System (EMS). The data traversing the switches provided real-time operational decision-making information and situational awareness. URE had identified and protected the switches as Cyber Assets within the Electronic Security Perimeter (ESP).

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE was affording the switches all the protections it provided to other CCAs and non-critical Cyber Assets within the ESP. Namely, the switches were behind firewalls in an ESP and surrounded in a six-wall enclosed Physical Security Perimeter (PSP). For those requirements for which the devices were unable to comply, there was an approved Technical Feasibility Exception (TFE) in place.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. performed a gap analysis to ensure it had properly classified all devices properly based on the present violation;
2. updated the CIP-002 list to show these devices;
3. ensured the senior manager approved the updated list; and
4. updated the ESP drawing to show the devices.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1 (SERC2013012691)

During a Compliance Audit, SERC determined that URE failed to identify all access points and Cyber Assets within the ESP. Specifically, URE failed to identify serial switches and one electronic access point (EAP) providing access to administrator workstations as access points to an ESP. The serial switches allow serial communications to traverse the ESP and communicate with the EMS. URE had

classified the devices as Cyber Assets within the ESP and protected them as such. The EAP at issue (a domain controller) was configured to allow virtual private network access from the corporate network and allowed remote personnel full administrative access on the ESP.

In addition, URE failed to identify an electronic access control and monitoring system and afford it the protective measures specified in CIP-005-3a R1.5. URE performed an EMS upgrade and failed to remove the domain controller from the ESP network.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to identify all access points and to protect Cyber Assets within the ESP could have resulted in vulnerabilities that allow a potential attacker to access and compromise systems within the ESP. Several factors mitigated the risk. First, the domain controller that remained within the ESP did not perform electronic access control for the newly deployed EMS. Second, URE has logging and monitoring enabled devices within the ESP that would have detected possible intrusion. Third, access to the devices was limited to authorized personnel who had completed cybersecurity training and had valid personnel risk assessments (PRAs). Finally, URE has a policy that prohibits personnel from connecting remotely to perform operational EMS functions.

URE's Mitigation Plan to address this violation was submitted to SERC.

URE's Mitigation Plan required URE to:

1. close all of the open network switch ports at all of its locations;
2. perform a gap analysis and update all of the required documents;
3. verify that all ports are monitored and alerted;
4. decommission the domain controller;
5. update the CIP-002 lists, which would then be approved by the senior manager;
6. test the switches for logging and alerting;
7. create a checklist for commissioning and decommissioning devices;
8. review the checklist with the appropriate personnel; and
9. design and implement an intermediate system.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1.4 (SERC2014013574)

URE submitted a Self-Report stating that it had failed to identify and protect all non-critical Cyber Assets within the ESP. During an internal review, URE discovered that it had not identified a printer and a tape library located within the ESP as Cyber Assets and therefore had not protected them under CIP-005-1 R1.4. The printer was in production before the date the Standard became mandatory and enforceable. URE added the tape library to the Cyber Asset list, protecting the device with compensating measures under CIP-005, removed the tape library from the inventory list 10 months later, but did not remove it from use. URE later determined that the tape library was required for proper management of backups and it remained in use; however, URE never added it back to the inventory list.

SERC determined that URE was in violation of CIP-005 R1.4 because it failed to identify and protect all non-critical Cyber Assets within the ESP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Compensating measures for the tape library remained in place during the entirety of the violation. The devices were peripherals that assist with user access and functionality but that could not affect the reliable operation of the BPS or perform any other essential functions within the ESP.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. created recurring tasks to review ports and services for the devices;
2. updated the Cyber Asset Inventory list to include the devices;
3. reviewed ports and services for the devices;
4. created a device commissioning checklist for devices installed in the ESP;
5. developed a process to scan periodically the network to determine if a device has been added or removed from inside the ESP;
6. tested and then implemented the new process;

7. reviewed security updates for each device;
8. applied all applicable updates; and
9. decommissioned the printer.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R3 (SERC2013011676)

SERC sent URE an initial notice of Compliance Audit. URE submitted a Self-Report stating that it was in violation of CIP-005-1 R3. SERC determined URE failed to implement electronic or manual processes for monitoring and logging at all access points to the ESP 24 hours a day, seven days a week.

Specifically, URE discovered access points, consisting of a firewall and front-end processors, which were not monitoring and logging. According to URE, when the devices were installed they were not properly configured to forward system and access logs to a centralized server that monitors system events related to cybersecurity. SERC verified that URE had a documented logging and monitoring process in place during the time of the violation.

SERC determined the duration of the violation to be from when URE installed the devices, through when URE configured the devices for monitoring and logging.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to monitor and log access to the access points could have resulted in unauthorized attempts to access the ESP without alerting URE. URE partially mitigated the risk because it configured its firewalls on the ESP to deny access by default, and all of the devices were located within an identified PSP with restricted access.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. configured the devices to send logs to the centralized server;
2. verified that the logs were being received; and
3. created a commissioning checklist to include configuration of monitoring methods.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R1 (SERC2013011702)

SERC sent URE an initial notice of Compliance Audit. URE submitted a Self-Report stating that it was in violation of CIP-006 R1. SERC determined URE failed to document the entry and exit of visitors from the PSP. During an approximately five-month period, URE employees escorted several visitors into the PSP without the escorts signing in the visitors using the required form. The employees escorted all the visitors while inside the PSP.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a Self-Report stating that it had also failed to create a completely enclosed six-wall border for all Cyber Assets within the ESP. URE discovered that one PSP had a clear opening of seven feet to the roof deck on top of several walls.

SERC determined the duration of the violation to be from when URE commissioned the PSP, through when URE completed the six-wall border.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. For the first instance, the escorts were authorized personnel with cybersecurity training and valid PRAs and escorted the visitors at all times while inside the PSP. For the second instance, to gain physical access to the PSP using the breach, an intruder would have to pass a guard, a mantrap, card readers, a biometric reader, and then climb to the breach. Finally, URE houses its CCAs within a six-wall cabinet with card access and a key lock.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. trained applicable personnel on the PSP procedures;
2. emailed all personnel regarding the importance of maintaining complete visitors logs at all PSP locations; and
3. installed a barrier in order to create a complete six-wall border.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R3 (SERC2013012693)

During a Compliance Audit, SERC determined that URE failed to implement technical controls to monitor for unauthorized access attempts to PSPs. While URE used alarm systems as its monitoring method for physical access, URE's alarms failed to provide immediate notification to personnel responsible for responding to unauthorized access attempts. In addition, URE had not configured one of the PSPs to process door forced open events. URE did have in place a documented process for monitoring physical access during the time of the violation.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to configure PSP access points for door forced open alarms could have allowed unauthorized access to the PSP to remain unnoticed and unchecked, potentially allowing malicious access to CCAs. However, personnel with the required cybersecurity training and PRAs man the first PSP continuously, and URE's PSPs had closed circuit television video monitoring at all access points.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. reconfigured and tested alarms/alerts at the affected PSPs;
2. developed a replacement checklist for quarterly and annual inspection; and
3. updated the applicable procedure and conducted training for the appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R1 (SERC2013012695)

During a Compliance Audit, SERC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls. URE was unable to provide the required test results for significant changes to new and to existing Cyber Assets within the ESP. URE had a documented process that required testing of all security-related changes to ensure that the change did not negatively affect or degrade existing cyber security controls. URE provided evidence that it performed some testing on some significant

changes; however, it was unable to provide evidence that all significant changes to new and existing Cyber Assets were adequately tested.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had conducted some testing on its Cyber Assets even though it failed to document the results for each test. Its process for testing significant changes to CCAs was to test the change on a quality assurance system before implementing the change on the production environment. Additionally, an ESP and PSP protected all CCAs, and all individuals with access to the CCAs had valid PRAs.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. developed a training PowerPoint, which emphasized the correct methods to identify significant changes;
2. provided the PowerPoint to the applicable personnel; and
3. created a form for documenting testing results.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R2: R2.1 (SERC2013012694)

During a Compliance Audit, SERC determined that URE failed to enable only those services required for normal and emergency operations. Specifically, one non-critical Cyber Asset, a server, had services enabled that were not required for normal and emergency operations. The services were part of the default installation for this particular device. URE had removed the services on other similar devices.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The device was a non-critical Cyber Asset that resided in an ESP, had no connectivity to outside networks, and could not control the BPS.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. reviewed and disabled the ports and services not required for normal and emergency operations;
2. developed differential scripts to track the before and the after regarding the removal of services and ports;
3. documented the changed services;
4. updated baseline documents for each device;
5. updated the change control procedure to require that scripts be run before and after major changes in order to detect unexpected alterations of ports and services; and
6. provided training to the applicable personnel on the updated change control procedure.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R3 (SERC2012009565)

URE submitted a Self-Report to SERC stating that it had failed to implement a patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the ESP. Specifically, 66% of its Cyber Assets were not included in its documented security patch management program. URE failed to apply patches and service packs to the Cyber Assets at issue.

While SERC was performing its assessment and determining the scope of the violation, it determined during a Compliance Audit that URE had also failed to assess some security patches within 30 calendar days of availability from the mandatory and enforceable date of this Standard until several years later. URE did not have a documented process for patch assessment for several years; however, URE did install some security patches during this period.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE updated the process to include all Cyber Assets, and assessed and installed all patches.

SERC determined that this violation posed a serious or substantial risk. Specifically, failing to assess and install security patches potentially exposed URE's CCAs to a number of vulnerabilities, which could

have allowed for a cyber-attack. URE did have some elements in place to protect these Cyber Assets. The Cyber Assets resided within a designated ESP and PSP, both of which required authorization for all individuals to access, and the Cyber Assets had antivirus software installed and monitored.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. assigned identifiers to each device to assist with tracking;
2. assessed all applicable patches;
3. assigned an additional employee to assist with patch implementation;
4. reviewed and updated the templates to supply patch assessment data; and
5. trained the applicable personnel on the updated template.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R4 (SERC2012009647)

URE submitted a Self-Report to SERC stating that it had failed to use antivirus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP. Specifically, it failed to install antivirus software or other malicious software tools on switches, routers, remote terminal units, and a digital video recorder. According to URE, these devices were not capable of running an antivirus or prevention tool; however, URE had not submitted a TFE.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a Self-Report stating that it had also failed to install antivirus software on certain CCAs. According to URE, it had installed a monitoring tool incorrectly believing the software was also antivirus and antimalware.

SERC determined the duration of the violation to be from when URE added the devices to production without antivirus software or other malware prevention tools, through when URE installed antivirus software on its systems.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to use antivirus software or malware prevention tools

could have allowed the introduction of malicious software to Cyber Assets exposing them to security vulnerabilities. URE had some elements in place that partially mitigated the risk. The systems were located inside an ESP and configured to send security and system logs to a central server for monitoring and alerting 24 hours a day, seven days a week. In addition, after installation of an antivirus software and a full scan, it was determined none of the systems contained viruses or malware.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. submitted TFEs for the devices that do not support antivirus; and
2. installed antivirus software on the missed devices.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R5 (SERC2012009566)

URE submitted a Self-Report to SERC stating that it had failed to establish and implement technical and procedural controls that enforce access authentication of and accountability for, all user activity and that minimize the risk of unauthorized system access. As part of its Cyber Vulnerability Assessment, URE discovered enabled user accounts on Cyber Assets within the ESP that it did not need for business purposes. Two were shared accounts, and the remaining accounts were local administrator accounts. These administrator accounts were not remotely accessible, and URE used them for the initial installation of vendor software. While SERC was determining the scope of the violation, URE submitted Self-Reports identifying additional issues.

URE failed to require passwords to meet the complexity requirements on 65% of its passwords. Specifically, the passwords were not technically capable of containing alpha, numeric, and "special" characters. URE had not submitted a TFE.

During a quarterly review, URE discovered that it failed to identify the individuals with access to the shared accounts. The accounts applied to network devices identified as CCAs.

URE failed to change default passwords on two Cyber Assets. URE had not checked to verify that it had changed the default accounts or passwords after vendor installation.

Finally, URE failed to change passwords at least annually as required. URE discovered over one hundred expired passwords on workstations. The workstations had a technical password control deployed to force a password change after 365 days; however, the control would only force a password change if there were an attempted login. There was no access to the accounts within the annual period, and the policy and control deployed did not enforce the annual change.

SERC determined the duration of the violation to be from when URE enabled accounts within the ESP that it did not need for business purposes, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to establish and implement procedural and technical controls for account management increased the risk of unauthorized access to CCAs and weakened the security of the ESP. However, all of the users had the required cybersecurity training as well as valid PRAs and URE protected all CCAs within an ESP and PSP.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. identified the devices with default accounts and removed, disabled, or modified them, as needed;
2. submitted a TFE with compensating measures for those devices that cannot meet password complexity requirements;
3. documented shared accounts for all devices within the ESP;
4. created a commissioning checklist for all devices installed inside an ESP; and
5. created a process to notify users of accounts with passwords that are nearing the 365-day age limit.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R6 (SERC2012009564)

URE submitted a Self-Report stating that it had failed to implement automated tools or organizational process controls to monitor cybersecurity system events on one or more Cyber Assets inside the ESP. Since their initial deployment, URE did not configure certain servers to send system logs to the centralized server.

While SERC was performing its assessment and determining the scope of the violation, URE submitted Self-Reports stating that it had also failed to review logs of system events related to cybersecurity and maintain records documenting reviewing logs. It failed to review manually event logs for two remote terminal units.

In addition, URE also failed to implement process controls to monitor system events for three Cyber Assets within the ESP. After URE generated log reports, it discovered the absence of logs for the three Cyber Assets. The devices were not technically capable of generating system event logs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE, through when URE configured the servers to forward logs.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to log and to monitor cyber system events could have allowed unauthorized access to Cyber Assets to be unnoticed and unchecked. Unauthorized access to its Cyber Assets within the ESPs could have resulted in an undetected security breach. An undetected security breach may have rendered CCAs inoperable, possibly resulting in the loss of monitoring and control of the BPS. However, the devices were all located within a designated ESP and PSP, and individuals with authorized access to the devices had an approved PRA and the required cybersecurity training. In addition, after review of the device logs, URE detected no significant cybersecurity events.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. identified all of the affected devices and configured them to forward logs to the centralized log server;
2. tested each device to verify that logs were being forwarded;
3. manually reviewed the logs of devices that cannot forward logs to the centralized log server; and
4. updated the TFEs for the devices that are unable to log.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of seventy thousand dollars ($70,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE had prior violation history, which was considered an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SERC considered a mitigating factor;
3. URE self-reported the violations of CIP-005-1 R1.4, and CIP-007-1 R3, R4, R5, and R6;
4. URE self-reported the violations of CIP-005-1 R3 and CIP-006-3c R1 after receiving notice of an upcoming Compliance Audit;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations of CIP-002-1 R3, CIP-005-1 R1.4, CIP-006-3c R1, and CIP-007-1 R1 and R2.1, posed a minimal risk, and the violations of CIP-005-1 R1, R3, CIP-006-1 R3, and CIP-007-1 R4, R5, and R6 posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
8. the violation of CIP-007-1 R3 posed a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of seventy thousand dollars ($70,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 10, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by SERC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seventy thousand dollars ($70,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	Sonia C. Mendonça* Deputy General Counsel, Vice President of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Marisa A. Sifontes* General Counsel Drew R. Slabaugh* Legal Counsel Rebecca A. Lindensmith* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 414-5244 (704) 414-5230 (704) 357-7914 – facsimile msifontes@serc1.org dslabaugh@serc1.org rlindensmith@serc1.org	James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Deputy General Counsel, Vice President of
Compliance and Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 31, 2015

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, D.C. 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP15-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The Spreadsheet NOP resolves 23 violations[4] of 12 Reliability Standards. In order to be a candidate for inclusion in the Spreadsheet NOP, the violations are those that had a minimal or moderate impact on the reliability of the bulk power system (BPS).

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).

[2] Attachment A is an excel spreadsheet.

[3] *See* 18 C.F.R § 39.7(c)(2).

[4] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. As designated in the attached spreadsheet, some of the Registered Entities have admitted to the violations, while the others have indicated that they neither admit nor deny the violations and have agreed to the proposed penalty as stated in Attachment A or did not dispute the violations and proposed penalty amount stated in Attachment A, in addition to other remedies and mitigation actions to mitigate the instant violations and ensure future compliance with the Reliability Standards. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

As discussed below, this Spreadsheet NOP resolves 23 violations. NERC respectfully requests that the Commission accept this Spreadsheet NOP.

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Text of the Reliability Standards at issue in the Spreadsheet NOP may be found on NERC's web site at http://www.nerc.com/page.php?cid=2|20. For each respective violation, the Reliability Standard Requirement at issue and the applicable Violation Risk Factor are set forth in Attachment A.

Unless otherwise detailed within the Spreadsheet NOP, the Registered Entities were cooperative throughout the compliance enforcement process; there was no evidence of any attempt to conceal a violation or evidence of intent to do so. In accordance with the Guidance Order issued by FERC concerning treatment of repeat violations and violations of corporate affiliates, the violation history for the Registered Entities and affiliated entities who share a common corporate compliance program is detailed in Attachment A when that history includes violations of the same or similar Standard. Additional mitigating, aggravating, or extenuating circumstances beyond those listed above are detailed in Attachment A.

Status of Mitigation[5]

The mitigation activities are described in Attachment A for each respective violation. Information also is provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order, the August 27, 2010 Guidance Order and the March 15, 2012 Compliance Enforcement Initiative Order,[7] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee. Such considerations include the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, the NERC Enforcement staff's review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the violations at issue.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[5] *See* 18 C.F.R § 39.7(d)(7).
[6] *See* 18 C.F.R § 39.7(d)(4).
[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Deputy General Counsel, Vice President of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Deputy General Counsel, Vice President of Compliance and Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

Attachment A

Spreadsheet Notice of Penalty
(Included in a Separate Document)

Attachment B

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY AND REGISTERED ENTITY SERVICE LIST FOR MARCH 2015 SPREADSHEET NOP FILING

FOR WECC:

Jim Robb
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6853
jrobb@wecc.biz

Michael Moon
Vice President Entity Oversight
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7608
(801) 883-6894 – facsimile
mmoon@wecc.biz

Ruben Arredondo
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7674
(801) 883-6894 – facsimile
rarredando@wecc.biz

Chris Luras
Director of Compliance Risk Analysis & Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

Attachment A-2

March 31, 2015 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

	A	B	C	D	E	F	G	H	I	J
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level
2	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013012654	Settlement Agreement	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-004-3a R2. WECC_URE1 issued temporary access badges to three employees so the employees could build a kitchen within a Physical Security Perimeter (PSP) where Critical Cyber Assets (CCA) were located. WECC_URE1's authorizing employee mistakenly believed that the three employees had received CCA training during the previous calendar year. However, the three employees last received CCA training two years prior. The three employees had physical access to eleven CCAs and one non-critical Cyber Asset at WECC_URE1's control center. As a result, WECC_URE1 was in violation of CIP-004-3a R2.1 for failing to ensure the three employees were trained prior to being granted access to the CCAs. The root cause of this violation was human error when WECC_URE1 verified the training dates for the three employees.	CIP-004-3a	R2	Lower	Severe
3	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2014013374	Settlement Agreement	WECC determined that WECC_URE1 was in violation of CIP-005-3a R2. WECC_URE1 performed troubleshooting that affected a router identified as an access point. During the troubleshooting, WECC_URE1 personnel issued a command that negated WECC_URE1's configured access list leaving the router without CIP-005 R2 controls. As a result, WECC_URE1 failed to use an access control model that denies access by default, such that explicit permissions were specified on the access point. WECC_URE1 also failed to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter (ESP) at one access point. The scope of this violation includes one access point and one ESP. The root cause of this violation was lack of training when conducting work on access points and by a lack of appropriately configured firewall that inherently denies access by default.	CIP-005-3a	R2	Medium	Severe
4	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2014013375	Settlement Agreement	WECC determined that WECC_URE1 was in violation of CIP-006-3a R2. WECC_URE1 failed to identify fourteen Cyber Assets that authorize and log access to the Physical Security Perimeter and afford them CIP protection outlined in Standard CIP-006-3a R2. WECC_URE1 has eleven Physical Access Control System (PACS) panels capable of providing access, monitoring, and logging independent of WECC_URE1's PACS servers. The control panels in scope are capable of controlling access to all fourteen of WECC_URE1's Physical Security Perimeters (PSPs). WECC_URE1 also has three workstations capable of provisioning access to all of WECC_URE1's PSPs. WECC_URE1 did not provide the eleven panels and three workstations all of the protections identified in CIP-006-3a R2. The root cause of this violation was WECC_URE1's misunderstanding of whether the devices in scope were subject to the Reliability Standards.	CIP-006-3a	R2	Medium	Severe
5	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2014013373	Settlement Agreement	WECC determined that WECC_URE1 was in violation of CIP-007-3a R8. Specifically, WECC_URE1 did not perform a Cyber Vulnerability Assessment (CVA) on each Cyber Asset in 2011 and 2012. Instead, WECC_URE1 used a representative system model to perform CVAs of representative devices. As a result, WECC_URE1 omitted 13 Cyber Assets from the 2012 CVA. Ten of the devices were Critical Cyber Assets (CCAs), two were non-critical Cyber Assets, and one was an Electronic Control and Monitoring device. WECC_URE1 also omitted 11 Cyber Assets from the 2011 CVA. Eight of the devices were CCAs, two of the devices were non-Critical Cyber Assets, and one of the devices was a Physical Access Control System device. The root cause of this violation was WECC_URE1's reliance on a representative system model to perform CVAs.	CIP-007-3a	R8	Lower	Severe

	K	L	M
1	Risk Assessment	Violation Start Date	Violation End Date
2	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE1 failed to ensure that three employees received training prior to being granted physical access to eleven CCAs and one non-CCA at WECC_URE1's control center. WECC_URE1's failure to train its employees on the proper use of Critical Assets increased the opportunity for the employees to improperly use the CCAs. Although WECC_URE1 granted access to the three employees, WECC_URE1 implemented preventive and detective controls. Specifically, WECC_URE1 implemented live video monitoring of the PSP 24 hours a day seven days a week. Additionally, each of the personnel involved in the violation had received prior CCA training. Furthermore, in this instance, the employees involved only had access to the PSP on a limited basis after receiving temporary access badges. Moreover, the PSP had a minimum of eight authorized, trained personnel inside at all times. The personnel and cameras minimized or prevented physical access to the CCAs and therefore would have prevented any unauthorized access to the supervisory control and data acquisition system.	when the three employees were granted access to the CCAs	when the three employees no longer had access to the CCAs
3	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. For three years, one WECC_URE1 access point lacked the protections required by CIP-005-3a R2.1 and R2.2. This exposed WECC_URE1 to the potential risk of unauthorized individuals using the unprotected access point to gain access to WECC_URE1's other devices and networks. Although one of WECC_URE1's access points lacked the protections required by CIP-005-3a R2.1 and R2.2, WECC_URE1 did implement and document organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP. Additionally, WECC_URE1 implemented a defense-in-depth architecture of physical and logical cyber security controls, including physical security mechanisms, special locks, and closed circuit television. WECC_URE1 also implemented internal cyber security controls including firewalls, vulnerability scanning tools, and a Security Information Events Management system.	when WECC_URE1 issued the command	when WECC_URE1 activated the Access Control List (ACL) on the router in scope
4	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE1 did not provide three workstations and eleven panels with all of the protections identified in CIP-006-3a R2 potentially exposing WECC_URE1's Critical Cyber Assets to access by unauthorized individuals. However, the panels in scope were protected by the inherent protections of the PACS network through WECC_URE1's PACS servers. WECC_URE1 installed the panels in either a PSP or a location protected from unauthorized physical access. WECC_URE1 also installed the workstations in either a PSP or located protected from unauthorized physical access, such as WECC_URE1 Central Monitoring Station or Badging Office. Furthermore, the 14 devices in scope were provided some of the protections identified in CIP-006-3a R2.2. Specifically, the panels and workstations were afforded the protections required by CIP-003 R1-R5, CIP-004, CIP-006 R4-R5, CIP-007 R7, and CIP-008.	when the Standard became mandatory and enforceable	Mitigation Plan completion
5	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE1 did not perform CVAs on all Cyber Assets in 2011 and 2012. This could have exposed WECC_URE1 to successful cyber-attacks against WECC_URE1's Cyber Assets. However, WECC_URE1 implemented compensating measures to decrease the risk associated with only performing CVAs on representative devices. Specifically, WECC_URE1 implemented a defense-in-depth architecture of physical and logical cyber security controls. This defense-in-depth architecture includes physical security mechanisms with guards, special locks, closed circuit television, and logical perimeter controls. WECC_URE1 also implemented internal cyber security controls including firewalls, vulnerability scanning tools, and a Security Information Events Management system. WECC_URE1 Tripwire reports also confirmed that the baselines of the devices in scope matched those of the representative devices.	when WECC_URE1 used the representative system model during the 2011 CVA	when WECC_URE1 performed the CVA on all required Cyber Assets

	N	O	P	Q	R	S	T
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
2	$65,000 (for WECC2013012654, WECC2014013374, WECC2014013375, and WECC2014013373)	Self-Report	To mitigate this violation, WECC_URE1: 1) started documenting the actual date of last CIP training in the Temporary Access Badge Log; 2) distributed a Bulk Operation Guide to all responsible senior load dispatchers responsible for issuing temporary badges and managing the Temporary Access Badge Log; 3) revised its Energy Control Centers (ECC) instructions for issuing temporary ECC badges that instructs entry of last CIP training date in the Temporary Access Badge Log; and 4) updated its training program for the load dispatcher with revised procedure related to issuing temporary ID badges for access to restricted areas of the ECC.	8/16/2013	12/20/2013	Neither Admits nor Denies	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE1's CIP-004 R2 compliance history to be an aggravating factor in the penalty determination.
3	$65,000 (for WECC2013012654, WECC2014013374, WECC2014013375, and WECC2014013373)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) activated the ACL on the router; 2) retrained its technical personnel on the proper procedure to follow when conducting work at non-firewall access point devices and to ensure that ACLs are reapplied once work is completed; 3) checked all Access Points for instances where non-firewall devices are used as access points and ensured that the device denies access by default; and 4) implemented a firewall that inherently denies access by default.	5/9/2014	11/21/2014	Neither Admits nor Denies	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
4	$65,000 (for WECC2013012654, WECC2014013374, WECC2014013375, and WECC2014013373)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) completed the change management form to include PACS workstations as devices afforded the protections of CIP-006 requirements (where applicable) and other requirements denoted in CIP-006 R2; 2) modified the change control management procedure and form to better detail when PACS devices must be added to the CIP Cyber Asset inventory; 3) reviewed the list of PACS devices to be afforded the protections of CIP-006 requirements (where applicable) and other requirements denoted in CIP-006 R2, verified the counts are correct and determined if Technical Feasibility Exceptions (TFEs) are required; 4) submitted TFEs (if required) to WECC; 5) developed an implementation schedule for bringing the PACS devices into compliance; 6) trained affected personnel on the modifications to the change control procedure; and 7) completed and signed off on change management forms demonstrating completion of implementation schedule for the PACS devices in scope.	11/12/2014	TBD	Neither Admits nor Denies	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
5	$65,000 (for WECC2013012654, WECC2014013374, WECC2014013375, and WECC2014013373)	Compliance Audit	To mitigate this violation, WECC_URE1: 1) assessed devices currently with Tripwire to assure that baselines of devices omitted from the CVA have no applicable deviation from the devices used as the representative sample when performing the CVA; 2) developed the WECC_URE1 plan for CVA requiring the individual testing of all devices and ensured all required activities were performed; 3) trained appropriate personnel on the new CVA plan; 4) implemented the new CVA plan against all required Cyber Assets; and 5) performed a quality assurance review for the implementation of the CVA Plan.	12/15/2014	TBD	Neither Admits nor Denies	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level
6	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013750	Settlement Agreement	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-003-3 R6. WECC_URE2 reported that its CIP-003-3 R6 procedure required the creation of a security control checkout form for every significant change. The security control checkout form documents a breakdown of how a significant change affects all applicable CIP-002 through CIP-009 requirements and ensures that all applicable CIP controls are applied prior to the change being put into production. WECC_URE2 reported there is no evidence of the form being created and filled out for the 23.85% change tickets that occurred in the year. WECC determined WECC_URE2 failed to follow its change control and configuration management process for 23.85% changes. WECC determined these changes affected 116 devices, and that the changes made by WECC_URE2 were patches and upgrades to servers, workstations, and other networking equipment. The root cause of the violation was WECC_URE2's failure to follow established procedures. Specifically, WECC_URE2 had inadequate oversight due to a lack of peer review or management review of change controls. WECC_URE2 did not have a dedicated quality assurance employee to verify results of change control. There was also a lack of training because some individuals did not know the change control and configuration management process.	CIP-003-3	R6	Lower	Severe
7	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013890	Settlement Agreement	During a Compliance Audit, WECC determined that WECC_URE2 was in violation of CIP-004-3a R4. WECC determined that on two occasions WECC_URE2 failed to revoke access to Critical Cyber Assets (CCAs) within seven calendar days for personnel who no longer require access to CCAs. In the first instance, a contractor no longer required access to WECC_URE2's CCAs. WECC_URE2 revoked access 28 days later. In the second instance, a WECC_URE2 employee verbally resigned. WECC_URE2 revoked access 14 days later. After the audit, WECC_URE2 reported a third instance of noncompliance. In that instance, a WECC_URE2 employee verbally resigned. WECC_URE2 revoked access 11 days later. The root cause of this violation was due to improper communication with vendors when a contractor has left employment and lack of management training and awareness regarding effect of certain human resources policies as applied to the voluntary separation of employees having access to a CIP environment.	CIP-004-3a	R4; R4.2	Lower	Moderate
8	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013503	Settlement Agreement	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-005-3a R5. WECC_URE2 made 13 changes to its networks or controls. The changes included adding and removing devices and updating firewalls. All 13 devices in scope are classified as Electronic Access Control and Monitoring devices responsible for protecting devices essential to a WECC_URE2 control center department. WECC_URE2 failed to update four pieces of documentation within 90 calendar days of the change. The root cause of this violation was WECC_URE2's failure to follow established procedures. Specifically, WECC_URE2 used a change control checklist, but the checklist did not include an explicit step to update relevant documentation as a result WECC_URE2 staff involved did not update relevant documentation.	CIP-005-3a	R5; R5.2	Lower	Severe
9	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013504	Settlement Agreement	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-006-1 R1. WECC_URE2 failed to conduct Cyber Vulnerability Assessments (CVAs) on 13 controls panels. WECC_URE2 never conducted full CVAs on three control panels. WECC_URE2 attempted to scan the three control panels, but the scan caused the control panels to crash. WECC_URE2's 16 control panels were not afforded the protective measures specified in Standards CIP-007-3 and CIP-009-3. WECC_URE2 also failed to verify that no default accounts resided on the panels on an annual basis. Additionally, two unauthorized personnel were left unescorted in an area containing WECC_URE2's Physical Access Control and Monitoring (PACM) server for the generating station's Physical Security Perimeters (PSPs) and a control panel. WECC also determined that WECC_URE2 failed to ensure that Cyber Assets that authorize or log access to the PSPs were protected from unauthorized physical access as required by CIP-006-3c R2.1. The root cause of this violation was equipment failure, lack of process and training issues as some of the WECC_URE2 personnel were not adequately trained on WECC_URE2's escorting procedures.	CIP-006-1	R1; R1.8	Medium	Severe

	K	L	M
1	Risk Assessment	Violation Start Date	Violation End Date
6	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE2's failure to follow its change control and configuration management process could allow for adding or modifying hardware and software changes that could compromise WECC_URE2's reliable operation of it transmission lines. Although WECC_URE2 failed to follow its change control and configuration management process, it did implement preventive controls. WECC_URE2 ensured that all CIP applicable devices resided within Electronic Security Perimeters (ESPs). WECC_URE2's devices were configured with tightly restricted ingress Access Control Lists and ports and services. WECC_URE2 disabled all dial-up access to assets within the ESP and required two-factor authentication for all external interactive access. WECC_URE2 also implemented detective controls. WECC_URE2 implemented Tripwire file integrity checker to verify no unauthorized functional changes occurred. Tripwire was configured to issue pop-up alerts to responsible personnel when a detected unauthorized change occurred. WECC_URE2 also conducted annual Cyber Vulnerability Assessments on all of its devices residing within an ESP. WECC_URE2's Cyber Vulnerability Assessment did not find any unaccounted ports and services or any default user accounts on the systems in scope. WECC_URE2 reviewed the security logs for these controls per CIP-007 R6 and it was determined that no malicious software was detected. Further, all personnel with access to Cyber Assets in the 23.85% change management tickets had CIP training and had current personnel risk assessments.	when WECC_URE2 failed to follow its change control process	Mitigation Plan completion
7	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to revoke access to CCAs in a timely manner could allow unauthorized individuals to have malicious physical access to WECC_URE2's CCAs. Although WECC_URE2 failed to revoke access to CCAs within seven calendar days, this violation was limited to three occasions that involved three individuals, none of whom were terminated for cause. WECC_URE2 verified the individuals did not attempt access after their separation. Additionally, the periods for these three occasions were of short duration, lasting 28 days, 14 days, and 11 days respectively. No harm is known to have occurred.	eight calendar days after the contractor in the first instance of noncompliance no longer required access	when WECC_URE2 terminated the employee's access in the third instance of noncompliance
8	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE2's failure to update relevant documentation after the 13 changes were made could have led to inaccurate documents that contain information regarding the CIP-005 protections of the Electronic Security Perimeters inside which the Critical Cyber Assets reside. Although WECC_URE2 failed to update the documentation, WECC_URE2 did implement preventive controls. WECC_URE2 followed all security related change controls when modifying, adding, or removing devices. As a result, devices were tested and approved prior to implementation of the change. No harm is known to have occurred.	91 calendar days after WECC_URE2 made changes to its network or controls	Mitigation Plan completion
9	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE2 uses the PACM devices in scope to implement physical controls required to protect WECC_URE2's devices. Unauthorized physical access to WECC_URE2's control panels could allow for physical compromise of the devices controlling all of WECC_URE2's transmission and generating systems which would affect WECC_URE2's peak load and generation. Although WECC_URE2 failed to ensure the 16 control panels classified as PACM devices were afforded the protective measures specified in CIP-006-3c R2, WECC_URE2 did implement preventive and detective controls. WECC_URE personnel responsible for recovering the devices were knowledgeable of the devices and had the vendors' contact information in the event the devices needed to be recovered. The control panels' functionality was limited by design which restricted malicious opportunities. Every year WECC_URE2 verified that no default accounts were enabled on the devices. WECC_URE2's PACM devices were all located in restricted facilities staffed 24 hours a day, seven days a week by personnel who only allowed access to authorized individuals. The two individuals left unescorted were discovered by staff who noticed the unescorted individuals and immediately notified WECC_URE2 management. WECC_URE2 confirmed that no harm occurred to the devices the unescorted individuals had access.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
6	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Self-Certification	To mitigate this violation, WECC_URE2: 1) created a security control checkout form training plan for the applicable group and delivered that training plan to the applicable group's quality assurance manager; 2) completed security checkout form documentation and training for the applicable group; and 3) completed security checkout form training for the applicable operations team. The training covered proper usage for the security checkout form as it relates to the NERC CIP-003-3 R6 process.	8/29/2014	TBD	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-003 compliance history to be an aggravating factor in the penalty determination.
7	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Compliance Audit	To mitigate this violation, WECC_URE2: 1) revised the separation and exit policy and procedures, along with accompanying supervisor's exit checklist, to provide emphasis on entering termination transactions early and adding language specific to NERC CIP areas; 2) incorporated the policy, including termination transactions and retirements, into periodic reminders sent to supervisors; 3) updated vendor contract language to comply with NERC Standards; and 4) reviewed master agreements and Individual Task Assignments for inclusion of the new language once the agreements expired.	2/16/2015	TBD	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-004 compliance history to be an aggravating factor in the penalty determination.
8	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Self-Certification	To mitigate this violation, WECC_URE2: 1) updated the four pieces of documentation; and 2) updated the checklist to include steps for updating documentation.	1/9/2014	10/20/2014	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's compliance history and determined there were no relevant instances of noncompliance.
9	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Self-Certification	To mitigate this violation, WECC_URE2: 1) met with the escort employee who did not follow procedures and retrained him on PSP escorting procedures; 2) revised the Emergency Situations section of the CIP Cyber Security Policy to ensure that the situation in question is adequately covered for future occurrences; 3) updated and installed new signage at the generating station data center PSP; 4) updated the process and/or any other processes deemed necessary to ensure that if an information security emergency occurs in a CIP-protected area, the CIP Cyber Security Policy's emergency must be followed; 5) updated the CIP Cyber Security Training course; 6) developed procedures for performing a CVA on the PACS field panels; 7) performed and documented the results of a CVA on the PACS field panels; 8) updated the Recovery Plan procedures to include the PACS field panels; and 9) conducted the annual Recovery Plan exercise to include PACS field panels, documented the results of the exercise, and reviewed meeting minutes.	8/30/2014	TBD	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-006-3c compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level
10	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013751	Settlement Agreement	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-007-3a R1. WECC_URE2 failed to implement the proper test procedures described in CIP-007-3a R1 for 31 change management tickets. The CIP-007 procedure states that a security control checkout form document is to be created for every significant change as this form helps ensures that all applicable CIP controls are applied, prior to the change being put into production. The security control checkout form was not filled out for the 31 significant change tickets. Further, WECC determined that WECC_URE2 were unable to confirm that testing was performed per the CIP-007 test procedure prior to the 31 significant changes being placed into production. These changes made by WECC_URE2 included patches and upgrades to servers, workstations, and other networking equipment that impacted 116 devices. The root cause of this violation was WECC_URE2's failure to follow established procedures. Specifically, WECC_URE2 had inadequate oversight due to a lack of peer review or management review of change controls. WECC_URE2 did not have a dedicated quality assurance employee to verify results of change control. There was also a lack of training because some individuals did not know the change control and configuration management process.	CIP-007-3a	R1	Medium	Severe
11	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013505	Settlement Agreement	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-007-3a R3. WECC_URE2's procedures required WECC_URE2 to review security patches within 30 days of their release and apply security patches within 90 days of their evaluation if the security patches are determined to be applicable. A Java patch was released and WECC_URE2 determined it was applicable and should be applied. Specifically, WECC_URE2 attempted to install the patch, but due to technical limitations the patch failed. Specifically, WECC_URE2 applied the patch to the workstation, but the update broke the Oracle Forms software. To fix this problem WECC_URE2 needed to install an update to the Oracle Forms on the backend server. The Oracle Forms update would not work until WECC_URE2 installed additional RAM on the backend server. WECC_URE2 did not install the Java patch until approximately three months after the patch should have been applied. The root cause of the violation was failure to include in its procedure a process to deal with software issues. WECC_URE2 had an established procedure, but waited too long to find a solution for the software issue so that it could follow its procedures within the 90 day time period.	CIP-007-3a	R3	Lower	Severe
12	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014013897	Settlement Agreement	During a Compliance Audit, WECC determined that WECC_URE2 was in violation of CIP-007-3a R8. WECC_URE2 failed to annually perform a Cyber Vulnerability Assessment (CVA) on all Cyber Assets in the Electronic Security Perimeters (ESPs) and failed to perform a complete CVA because not all ports and services on all Cyber Assets were assessed. WECC_URE2 used ports and services information gathered from one Cyber Asset as a representative sample to satisfy the vulnerability for 38 other Cyber Assets. WECC_URE2 only scanned one device to collect current ports and services information and the information was gathered from a test system and not from the actual Cyber Assets in question. WECC_URE2 also failed to gather current ports and services information from an additional 23 Cyber Assets. This led to a violation that included 21 Critical Cyber Assets (CCAs) and 41 non-critical Cyber Assets. The root cause of the violation was a process deficiency. Specifically, the technical team involved was not able to perform the CVA scan due to device and system outage limitations and felt that a scan on a representative sample would be sufficient.	CIP-007-3a	R8; R8.2; R8.3	Lower	Severe

	K	L	M
1	Risk Assessment	Violation Start Date	Violation End Date
10	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE2's failure to complete its security check out form could have allowed for the adding or modifying hardware and software changes that are harmful to Critical Cyber Assets essential to the operation of the BPS. Although WECC_URE2 failed to complete its security check out form, WECC_URE2 did implement preventive controls. WECC_URE2 ensured that all CIP applicable devices resided within Electronic Security Perimeters (ESPs). WECC_URE2's devices were configured with tightly restricted ingress Access Control Lists and ports and services. WECC_URE2 also disabled all dial-up access to assets within the ESP and required two-factor authentication for all external interactive access. WECC_URE2 also implemented detective controls. WECC_URE2 implemented Tripwire File Integrity Checker to verify no unauthorized changes occurred. Tripwire File Integrity Checker was configured to issue pop-up alerts to responsible personnel when a detected unauthorized change occurred. WECC_URE2 also conducted annual Cyber Vulnerability Assessments (CVA) on all its devices residing within an ESP. WECC_URE2's CVA did not detect any unaccounted ports and services or any default user accounts on the systems in scope. WECC_URE2 reviewed the security logs for these controls per CIP-007 R6 and it was determined that no malicious software was detected. Further, all personnel with access to Cyber Assets in the 31 change management tickets had CIP training and had current personnel risk assessments.	when WECC_URE2 first failed to follow proper test procedures	Mitigation Plan completion
11	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE2's failure to install the patch impacted one workstation used by the operators to control WECC_URE2's energy management system (EMS). This failure could have allowed vulnerabilities on the workstation to remain unnoticed and unchecked for a longer duration. Although WECC_URE2 failed to install the patch within 90 days, WECC_URE2 did implement compensating controls. WECC_URE2 was aware of the patch and the associated vulnerabilities addressed by the patch. WECC_URE2 did install the patch as soon as technically feasible. The Electronic Security Perimeter (ESP) for the EMS is protected behind a Physical Security Perimeter with adequate controls, monitoring, and logging in accordance with CIP-006 R4, R5, and R6. All Cyber Assets within the ESP are protected with antivirus and anti-malware controls. WECC_URE2 reviewed the security logs for these controls per CIP-007 R6 and it was determined that no malicious software was detected. Finally, all personnel with access to the Windows workstation had CIP training and had current personnel risk assessments.	91 days after WECC_URE2 determined the Java patch was applicable	when WECC_URE2 installed the Java patch
12	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, WECC_URE2's failure to conduct CVAs on 21 CCAs and 41 non-critical Cyber Assets led to a situation where WECC_URE2 put the 62 Cyber Assets at risk of compromise and unauthorized manipulation. Although WECC_URE2 failed to conduct the CVAs, WECC_URE2 did implement compensating measures. WECC_URE2 implemented a defense-in-depth strategy including physical and logical cyber security controls such as physical security mechanisms with guards and closed-circuit television. WECC_URE2 also implemented logical perimeter and other cyber security controls including firewalls, intrusion detection systems, and least-privilege account management practices.	the day after WECC_URE2 completed its Mitigation Plan for a prior violation of this Standard	present

	N	O	P	Q	R	S	T
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
10	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Self-Certification	To mitigate this violation, WECC_URE2: 1) configured Tripwire Enterprise System to show all applicable security controls have been tested and passed to prevent occurrence of similar future issues; 2) created security control checkout form training plan for the applicable group and delivered it to the applicable group's manager; 3) completed security control checkout form documentation and training for the applicable group; and 4) completed security control checkout form training for the operations team.	8/29/2014	TBD	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-007 compliance history to be an aggravating factor in the penalty determination.
11	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Self-Certification	To mitigate this violation, WECC_URE2: 1) upgraded server memory to allow for successful back-end application updates; 2) upgraded Oracle Forms and performed Java updates; 3) documented the update in the CIP-007-3 R3 patch tracking spreadsheet; 4) updated the Technical Feasibility Exception (TFE) template to reflect different TFE options; and 5) trained operations IT subject matter experts on the new procedure.	6/26/2014	11/24/2014	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-007 compliance history to be an aggravating factor in the penalty determination.
12	$85,000 (for WECC2014013750, WECC2014013890, WECC2014013503, WECC2014013504, WECC2014013751, WECC2014013505, and WECC2014013897)	Compliance Audit	To mitigate this violation, WECC_URE2 will: 1) begin to transition to compliance with some or all of the CIP V5 Standards; 2) split the entire network to where all in-scope systems will be on two separate networks, two in each network; and 3) declare all Cyber Assets and systems at the generating facility to be part of one or more low impact Bulk Electric System cyber systems (LIBCS), as a result the LIBCS at the facility will no longer be in scope for any requirements pertaining to the execution of a CVA.	11/5/2014	TBD	Neither Admits nor Denies	WECC reviewed WECC_URE2's internal compliance program and considered it to be a mitigating factor in the penalty determination. WECC considered WECC_URE2's CIP-007 compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level
13	Western Electricity Coordinating Council (WECC)	WECC_URE3	NCRXXXXX	WECC2014014001	Settlement Agreement	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-007-3a R6. WECC_URE3 reported that it failed to ensure that all Cyber Assets within the Electronic Security Perimeter (ESP) implemented automated tools or organizational process controls to monitor system events that are related to cyber security, as required by CIP-007-3a R6. Specifically, WECC_URE3 failed to properly maintain and review logs for three Supervisory Control and Data Acquisition (SCADA) switches and to retain logs for 90 days for two Energy Management System (EMS) servers. As a result, WECC_URE3 reported that it had a violation of CIP-007-3a R6. WECC determined that WECC_URE3 failed to ensure that all Cyber Assets within the ESP implemented automated tools or organizational process controls to monitor system events that are related to cyber security, as required by CIP-007-3a R6. The root cause involving the three switches was human error in that one employee did not add the devices to the Security Incident and Event Management (SIEM) for monitoring. The root cause for the servers not retaining 90 days worth of logs was due to technical errors as a result of a mis-configuration after a re-installation on a client after testing was performed.	CIP-007-3a	R6; R6.4; R6.5	Lower	Severe

	K	L	M
1	Risk Assessment	Violation Start Date	Violation End Date
13	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE3 failed to implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, WECC_URE3 failed to maintain and review logs for three SCADA switches which provide internal communication between SCADA workstations and SCADA servers. WECC_URE3 also failed to retain logs for 90 days for two EMS servers. Failing to implement, maintain, and review a logging system and failing to retain logs for 90 days could lead to undetected security incidents. A malicious person could scan these devices to discover vulnerable ports and services and launch an attack against any discovered vulnerabilities. WECC_URE3 implemented strong preventative controls to prevent undetected security incidents from occurring. Specifically, WECC_URE3 configured the operating system on these switches to limit which ports and services are allowed to open and start prior to adding them to the ESP. In other words, this configuration restricts any unauthorized ports and services outside of their current configuration, reducing the likelihood of an unauthorized user from leveraging a vulnerable port or service and gaining remote access to the SCADA switches. WECC_URE3 also implemented strong detective controls to detect any security incidents. Specifically, WECC_URE3 implemented a SIEM device that is used to monitor the logs of the SCADA devices. If someone were to gain control of the switches and attempt to then gain control of other SCADA devices, the security information and event management (SIEM) could detect that attempt. Since the SIEM monitors the SCADA devices 24 hours per day, seven days a week, an email would have been sent to security personnel alerting them about an unauthorized access attempt. The security personnel on-call would likely investigate, review the logs, and determine the unauthorized ports and services to shut them down. This would stop the network connection of the unauthorized personnel by shutting down the unauthorized ports and services, preventing unauthorized access to the SCADA devices. As further compensation, WECC_URE3 implemented strong compensating controls. Specifically, WECC_URE3 implemented a Cisco operating system (IOS) configuration to prevent unknown Media Access Control (MAC) addresses from connecting to the network. This MAC address restriction would likely prevent remote logging into the SCADA switches and attempt to access other SCADA devices. WECC_URE3 implemented additional strong compensating controls. Specifically, WECC_URE3 implemented locks on cabinets that contain these switches which would likely prevent a malicious person from physically damaging the three switches in scope. The locked cabinets prevent employees from getting physical access to the switches and not be able to access the switches via a serial cable and its console port. WECC_URE3 also added a firewall to restrict network access within the ESP and provide access point protections.	the date that WECC_URE3 put the switches into production without the appropriate monitoring tools	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
13	$15,000	Self-Report	To mitigate this violation, WECC_URE3: 1) WECC_URE3 submitted evidence of the new switches being added as data sources within its SIEM and its log collection occurring; and 2) WECC_URE3 configured the alarm/notification to notify WECC_URE3 personnel when a “data source” client has stopped forwarding logs.	8/1/2014	11/14/2014	Does Not Contest	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

April 30, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into Settlement Agreements to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreements, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

the terms and conditions of the Settlement Agreements. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the two Settlement Agreements, one resolving 15 CIP violations and the second resolving 3 TOP-006-2 violations. The details of the findings and basis for the penalty are set forth in the Settlement Agreements and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreements by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreements, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013013201	CIP-005-1	R1: R1.5	Medium/ Severe	$150,000
RFC2013013202	CIP-005-1	R2: R2.1, R2.2	Medium/ Severe	
RFC2013013203	CIP-005-1	R3: R3.2	Medium/ Severe	
RFC2013013204	CIP-005-1	R4	Medium/ Severe	
RFC2013013205	CIP-006-1	R1:R1.8	Medium/ Severe	
RFC2013013206	CIP-007-1	R1	Lower/ Severe	
RFC2013013207	CIP-007-1	R2: R2.1, R2.2	Medium/ Severe	
RFC2013013208	CIP-007-1	R3: R3.2	Lower/ Severe	
RFC2013013254	CIP-007-3a	R3	Lower/ Severe	
RFC2013013209	CIP-007-1	R4: R4.1	Medium/ Severe	
RFC2013013210	CIP-007-1	R5: R5.1.2, R5.2	Medium/ Severe	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
RFC2013013211	CIP-007-1	R6: R6.1, R6.2, R6.4, R6.5	Medium/ Severe	$150,000
RFC2013013212	CIP-007-1	R7	Lower/ Severe	
RFC2013013213	CIP-007-1	R8: R8.1, R8.2, R8.3	Medium/ Severe	
RFC2013013214	CIP-009-1	R5	Lower/ Severe	
RFC2013013251	TOP-006-2	R1	Medium/ Severe	
RFC2013013252	TOP-006-2	R2	High/ Severe	
RFC2013013253	TOP-006-2	R5	Medium/ Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

Background

ReliabilityFirst conducted a Compliance Audit of URE (Compliance Audit), during which ReliabilityFirst discovered 14 violations of the CIP Reliability Standards. In addition, URE submitted four Self-Reports to ReliabilityFirst stating it was in violation of CIP-007 R3 and TOP-006-2 R1, R2, and R5. ReliabilityFirst and URE negotiated the subject matter of two Settlement Agreements simultaneously, and the penalty associated with the CIP Settlement Agreement includes the assessment of the three TOP-006 violations. NERC staff determined that it was appropriate to process the two separate agreements as a single non-public Notice of Penalty because the facts and circumstances of the three TOP-006-2 violations stemmed directly from the CIP-007 R3 violation.

ReliabilityFirst determined that all of the violations at issue in this Agreement, taken together, except CIP-007-1 R7, posed a serious and substantial risk to reliability. However, ReliabilityFirst determined that it was not necessary to issue a Remedial Action Directive for the violations because URE immediately designed an aggressive, comprehensive Mitigation Plan through which it adopted an entirely new CIP Compliance Program, as described in further detail in the Settlement Agreements.

ReliabilityFirst determined that at the time these violations occurred, URE lacked subject matter experts trained in CIP compliance, and the entity's operating personnel were not required to observe or were not aware of the applicable compliance practices. ReliabilityFirst determined that insufficient management oversight contributed to these issues. ReliabilityFirst determined that if URE had

performed certain key management practices, especially risk management, URE could have reduced the number and severity of its violations.

URE submitted its Mitigation Plan to address the CIP violations to ReliabilityFirst. URE recognized the severity of the risk posed by the subject violations and designed a single, holistic Mitigation Plan that encompassed all of the violations. URE implemented an entirely new CIP Program rather than attempting piecemeal mitigation of the noncompliance. URE has taken certain actions in this Mitigation Plan that address compliance with the multiple violations at once. URE's Mitigation Plan required URE to:

1. verify its Critical Cyber Asset (CCA) inventory by performing a physical walk-down of all Electronic Security Perimeters (ESPs);
2. conduct training for URE staff on revised policies and procedures, including creating and maintaining detailed review and approval schedules for compliance documents;
3. ensure all personnel attend training sessions to discuss the redesigned policies and procedures which apply to their functional areas;
4. reinforce new procedural tasks through task execution; and
5. identify key individuals who will serve as primary points of contact for questions regarding modified policies and procedures.

URE certified that the above Mitigation Plan requirements were completed.

This Full Notice of Penalty will address the portions of the Mitigation Plan that address each of the specific individual violations within the description of each violation below.

CIP-005-1 R1 (RFC2013013201)

During the Compliance Audit, ReliabilityFirst determined that URE failed to provide adequate protection to electronic access control and monitoring (EACM) Cyber Assets engaged in the access control or monitoring of an ESP. Specifically, URE failed to provide the following protective measures of CIP-007: cyber security testing procedures (R1), security patch management (R3), account management (R5.1.2, R5.2.1, R5.2.2, and R5.2.3), EACM disposal or redeployment procedures (R7), and Cyber Vulnerability Assessments (CVAs) (R8.1, R8.2, and R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through the date URE completed its mitigating actions for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the risk was increased because URE had no compensating measures in place and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. document and implement all procedures related to the referenced requirements of cyber security testing procedures (R1), security patch management (R3), account management (R5.1.2, R5.2.1, R5.2.2, and R5.2.3), EACM disposal or redeployment procedures (R7), and CVAs (R8.1, R8.2, and R8.3); and
2. ensure that all EACMS are appropriately included in the scope of these procedures as they are completed in the remaining steps of this Mitigation Plan.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (RFC2013013202)

During the Compliance Audit, ReliabilityFirst determined URE failed to provide adequate evidence of documented organizational processes for control of electronic access at all electronic access points to the ESP. First, URE did not have a documented organizational process for controlling electronic access at all electronic access points to the ESP by enabling only ports and services required for operations and monitoring. Second, URE disallowed inbound traffic through its firewall, but outbound Internet Protocol traffic was set to "permit by default" rather than "deny by default" (R2.1). Third, URE did not enable only ports and services required for operations and for monitoring Cyber Assets within the ESP (R2.2).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through the date URE completed its mitigating actions for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to limit routable communication across the access points to the ESP weakened the defense required for protection of CCAs. URE did not restrict outbound traffic from one of its ESPs, creating the opportunity for a compromised asset to communicate freely with a command and control server or other non-approved device. URE had no compensating measures in place, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. ensure that all ESP access points are configured to deny access by default;

2. document and implement procedures to ensure compliance with CIP-005 R2;
3. clearly document operational necessity for ports and services at ESP access points; and
4. revise access point configuration to limit ports and services to only those required.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R3 (RFC2013013203)

During the Compliance Audit, ReliabilityFirst determined URE failed to have a documented process for monitoring and logging access at access points to the ESP. In addition, URE did not monitor attempts at or actual unauthorized accesses (R3.2) and only monitored failed login attempts.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to monitor and log access to an ESP can result in undetected attacks on the ESP and undetected compromise of assets within the ESP. Failure to alert on unauthorized access attempts may result in an insufficient or untimely response to attacks on the ESP. URE had no compensating measures in place to reduce these risks, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-005 R3;
2. develop and implement a procedure to monitor system events related to cyber security;
3. ensure each ESP access point is configured for security event logging and monitoring;
4. verify that all Cyber Assets within an ESP are adequately monitored for security events, and verify the configuration of automated or manual alerts for systems related to its energy control system (ECS);
5. ensure alerts are generated for unauthorized access attempts and actual unauthorized access; and
6. maintain logs relating to system events for ECS, as well as evidence of the log reviews for ninety calendar days.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (RFC2013013204)

During the Compliance Audit, ReliabilityFirst determined URE failed to include all required elements in its CVAs. URE's annual CVA did not include a review of ports and services (R4.2), discovery of access points to the ESP (R4.3), and a review of controls for default accounts, passwords, and network management community strings (R4.4). In addition, URE did not have a document identifying the CVA process (R4.1) or clear documentation of the results of the CVAs (R4.5).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to perform an adequate CVA kept URE from examining its security practices and identifying necessary improvements. URE had no compensating measures in place, and the violation lasted for a prolonged period.

URE's Mitigation Plan required URE to:

1. implement procedures to ensure compliance with CIP-005 R4;
2. document clearly that an annual CVA has been performed;
3. verify that the annual CVA includes all Cyber Assets within the ESP(s), EACMs, Physical Access Control Systems (PACS) and access points and that only ports and services required for operation are enabled;
4. document clearly a review of controls for default accounts and verify that the annual CVA includes a review of ports and services, discovery of access points to the ESP, and a review of controls for default accounts, passwords, and community strings; and
5. document the results of the CVA and an action plan to address findings.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-1 R1.8 (RFC2013013205)

During the Compliance Audit, ReliabilityFirst determined URE failed to provide adequate protective measures for Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP). URE failed to afford its PACS that authorize and/or log access to the PSPs the following protective measures of CIP-007: cyber security test procedures (R1.3), ports and services processes (R2.1 and

R2.2), security patch management (R3.2), account management (R5.1.2, R5.2.1, and R5.2.3), security status monitoring (R6.1), and CVAs (R8.1, R8.2, and R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the Cyber Assets at issue could be compromised allowing unauthorized access to the CCAs and PSPs. Although the PACS did not reside within the ECS ESP, the PACS did reside within the URE corporate network, which the corporate internal and external intrusion prevention systems protected. The PACS was also behind the corporate firewall, which has a deny-all rule in place as a default. Finally, URE utilized a managed security service provider for the PACS to establish a method of generating and maintaining logs of sufficient detail to create historical audit trails of individual user access activity for a minimum of ninety days.

URE's Mitigation Plan required URE to:

1. document and implement all procedures related to the requirements referenced in CIP-006-3 R2.2; and
2. ensure that all PACS are appropriately included in the scope of these procedures.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R1 (RFC2013013206)

During the Compliance Audit, ReliabilityFirst determined URE failed to create, implement, and maintain cyber security test procedures for all Cyber Assets within the ESP, document that it performs testing that reflects the production environment, and document the test results. URE did not have a clearly defined test procedure for Cyber Assets within the ESP (CIP-007-1 R1.1) and EACM Cyber Assets (CIP-005-1 R1.5). URE did not clearly document that it performed testing in a manner that reflected the production environment (CIP-007-1 R1.2). URE did not document test results for new Cyber Assets and significant changes to existing Cyber Assets within the ESP (CIP-007-1 R1.3), EACM Cyber Assets (CIP-005-1 R1.5), and Cyber Assets that authorize and/or log access to the PSP (CIP-006-3c R2.2).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, inadequate testing of the impact of changes on cyber security controls exposed protected assets to higher risk of compromise. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R1 by creating, implementing, and maintaining adequate test procedures for all Cyber Assets residing within the ESP, EACMs, and PACS;
2. test procedures to ensure testing of security controls required by CIP-005-3 and CIP-007-3; and
3. document that testing performed is representative of the production environment.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R2 (RFC2013013207)

During the Compliance Audit, ReliabilityFirst determined URE failed to establish, document, and implement a process to ensure only those ports and services required for normal and emergency operations are enabled for Cyber Assets within the ESP (CIP-007-1 R2) and Cyber Assets that authorize and/or log access to the PSP (CIP-006-3c R2.2). Accordingly, URE failed to enable only those ports and services required for normal and emergency operations and disable other ports and services.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failing to keep the number of listening ports and active services at a minimum exposed URE's Cyber Assets to a greater risk of compromise. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R2;
2. document clearly that only ports and services required for normal and emergency operations are enabled for all Cyber Assets within the ESP; and
3. document clearly that ports and services not required for operations or monitoring are disabled prior to production use.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-3 R3 (RFC2013013208)

During the Compliance Audit, ReliabilityFirst determined URE failed to implement a patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for Cyber Assets within the ESP. URE also failed to provide sufficient evidence of the implementation of security patches for Cyber Assets within the ESP, EACM devices, and PACS devices. URE did not monitor certain sources of software patches for Cyber Assets within the ESP, EACM devices, and PACS devices.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, failure to implement properly a security patch management system made URE vulnerable to infiltration from outside entities. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. document clearly the assessment of all security patches for all applicable assets and for all applicable patch sources as required; and
2. schedule security patches for installation in accordance with URE policy.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R4 (RFC2013013209)

During the Compliance Audit, ReliabilityFirst determined URE failed to use antivirus software or malicious software prevention tools on all Cyber Assets within the ESP. In addition, URE failed to document and implement antivirus and malware prevention tools and failed to document and implement compensating measures used to mitigate risk exposure in cases where it did not install antivirus software and malware prevention tools.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the failure left the organization vulnerable to viruses and malware. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R4;
2. document clearly that antivirus software and malicious software prevention tools are used on all Cyber Assets within the ESP; and
3. develop and implement compensating and mitigation measures for those Cyber Assets that are not capable of running antivirus or malware prevention tools.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R5 (RFC2013013210)

During the Compliance Audit, ReliabilityFirst determined URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. ReliabilityFirst identified four instances of noncompliance. First, URE provided evidence that it was logging security events, but URE failed to create historical audit trails of individual account access activity (R5.1.2). Second, for Cyber Assets within the ESP, EACM devices, and PACS devices, URE failed to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges (R5.2). Third, for Cyber Assets within the ESP and EACM devices, URE failed to identify individuals or roles with access to shared accounts (R5.2.3). Finally, for Cyber Assets within the ESP and EACM devices, URE failed to establish an audit trail of shared account use or steps for securing the account in the event of personnel changes (R5.2.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE's failures increased the likelihood for unauthorized system access and decreased the likelihood that URE would detect an unauthorized system access. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R5;
2. document clearly historical audit trails for individual user account access activity for Cyber Assets, EACMs, and PACs;
3. develop and implement a policy that minimizes and manages the scope and acceptable use of administrative, shared, and other generic account privileges; and
4. document clearly audit trails of account use and the procedural steps to secure the accounts in the event of personnel changes.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R6 (RFC2013013211)

During the Compliance Audit, ReliabilityFirst determined URE failed to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor cyber security-related system events for approximately four years. In addition, URE failed to ensure that all Cyber Assets within an ESP were monitoring for security events (R6.1) and failed to configure monitoring systems to issue automated or manual alerts for ECS (R6.2). Furthermore, URE failed to demonstrate that it retained logs for 90 calendar days (R6.4) and failed to provide evidence of the review of logs related to system events for ECS (R6.5).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE's failure to monitor cyber security-related system events decreased the likelihood that URE would detect a potential compromise on the system. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R6;
2. develop and implement a procedure to monitor system events related to cyber security;
3. ensure that each ESP access point is configured for security event logging and monitoring;
4. verify that all Cyber Assets within an ESP are adequately monitored for security events;

5. verify the configuration of automated or manual alerts for ECS;
6. ensure alerts are generated for unauthorized access attempts and actual unauthorized access; and
7. maintain logs relating to system events for ECS, as well as evidence of the log reviews, for 90 calendar days.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R7 (RFC2013013212)

During the Compliance Audit, ReliabilityFirst determined URE failed to establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP. URE provided a policy, which stated URE has established formal methods, policies, and procedures for disposal of Cyber Assets within the ESP. However, the policy did not provide such methods, policies, and procedures.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Despite not having formal documentation in place, URE was disposing of and redeploying Cyber Assets within the ESP according to the Standard. URE kept assets removed from service in a physically secure environment. While URE did not maintain an inventory list, there was restricted access to the area where the equipment was being stored, and URE developed an inventory list prior to sending any items for destruction.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-007 R7; and
2. develop and implement formal disposal or redeployment processes and procedures for Cyber Assets within the ESP.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-1 R8 (RFC2013013213)

During the Compliance Audit, ReliabilityFirst determined URE failed to document its CVA process for one year (R8.1), conduct a review to verify that only ports and services required for operation are enabled (R8.2), and conduct a review of controls for default accounts (R8.3).

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, URE did not have sufficient awareness of the vulnerabilities of its ESP access points or Cyber Assets within the ESP, and therefore was more vulnerable to attack. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-005 R4 and CIP-007 R8;
2. document clearly that an annual CVA has been performed;
3. verify that the annual CVA includes all Cyber Assets within the ESP(s), EACMs, PACs and access points and that only ports and services required for operation are enabled;
4. document clearly a review of controls for default accounts and verify that the annual CVA includes a review of ports and services, discovery of access points to the ESP, and a review of controls for default accounts, passwords, and community strings; and
5. document the results of the CVA and draft an action plan to address findings.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-009-1 R5 (RFC2013013214)

During the Compliance Audit, ReliabilityFirst determined URE failed to demonstrate it annually tested the backup media containing information essential for the recovery of CCAs. For its ECS operations area, URE had a procedure to perform information backups on various types of CCAs, but URE failed to demonstrate it annually tested its backup media that contains information essential for the recovery of CCAs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, while URE had information essential to the recovery of CCAs on backup media, URE did not test the backup media annually and had no assurance that it could use this backup media to recover CCAs if necessary. URE had no compensating measures in place to reduce this risk.

URE's Mitigation Plan required URE to:

1. develop and implement procedures to ensure compliance with CIP-009 R5; and
2. conduct and clearly document an annual test of backup media that contains information essential for the recovery of CCAs.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-007-3a R3 (RFC2013013254), TOP-006-2 R1 (RFC2013013251), R2 (RFC2013013252), and R5 (RFC2013013253)

URE submitted four Self-Reports to ReliabilityFirst stating it had violations of CIP-007-3a R3 and TOP-006-2 R1, R2, and R5. A URE transmission operations control center (TOCC) experienced an ECS failure lasting approximately 91 minutes during which the TOCC lost monitoring and control capabilities. The root cause of this particular service interruption was that URE had not assessed an upgrade released at the time of the ECS outage. Following the ECS outage and the Compliance Audit, URE discovered that it evaluates antivirus software patches, but does not track, evaluate, test, and install all software patches (R3). In addition, URE did not satisfactorily identify and describe compensating measures applied to mitigate risk exposure when it fails to install a security patch.

URE violated TOP-006-2 R1 by failing to monitor the status of all transmission resources available for use and failed to inform the Reliability Coordinator of all available transmission resources. URE violated TOP-006-2 R2 by failing to monitor applicable transmission line status, real and reactive power flows, voltage, and status of rotating and static reactive resources. URE violated TOP-006-2 R5 by not using monitoring equipment to communicate to operating personnel any important deviations in operating conditions and to indicate, if appropriate, the need for corrective action.

ReliabilityFirst determined the duration of the CIP-007-3a R3 violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed its mitigating activities for this violation.

ReliabilityFirst determined the duration of the three TOP-006 violations to be 91 minutes on the day of the incident, when it lost the ability to monitor due to the ECS failure.

ReliabilityFirst determined that this violation posed a serious or substantial risk. Specifically, the inadequately tested patch caused a service interruption for approximately 91 minutes. There was no real-time, accurate data for URE to transmit due to the ECS issues. URE lost BPS visibility and monitoring for approximately 91 minutes.

Throughout the event, URE maintained communication with its Reliability Coordinator, neighboring Transmission Operators, and all URE generating plants to ensure monitoring of the system. The interconnecting Transmission Operators monitored the URE system during the event. URE followed its emergency operating plans for loss of control center functionality to assess and respond to the event.

URE mitigated the CIP-007 R3 violation through the holistic CIP Mitigation Plan with the same actions as listed above in the CIP-007 R3 (RFC2013013208) description.

URE's Mitigation Plan to address the TOP violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. develop a plan to assess and improve the backup control center functionality, including developing a plan to connect remaining non-critical Remote Terminal Units to the backup ECS and install backup communications system hardware, including fiber optic cables;
2. include in the plan automating steps to transfer communications to backup control centers;
3. enhance synchrophasor usage, including adding phasor data collector server hardware at the backup control center, fully replicating synchrophasor functionality at the backup control center, and creating user screens and views to enhance situational awareness;
4. add redundant synchrophasor monitoring replicating the primary control center, which when acting together with automating communications to the backup control center, will reduce time delays to disable the primary system and activate the backup system as well as increase operators' situational awareness;
5. provide training to its TOCC operators relating to synchrophasors; and
6. review and improve operations technology on-call and operator procedures, enhance the ECS dashboard, and train operations technology support and TOCC operators on revised procedures and the ECS dashboard.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreements, ReliabilityFirst has assessed a penalty of one hundred fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations which ReliabilityFirst considered a mitigating factor;
3. URE self-reported the violations of CIP-007-3a R3 and TOP-006-2 R1, R2, and R5;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. ReliabilityFirst determined that the violations, considered together (with the exception of CIP-007-1 R7), posed a serious and substantial risk to the reliability of the BPS and indicated a systematic performance failure by URE;
7. URE committed to a comprehensive Mitigation Plan with an aggressive completion schedule. URE also agreed to complete significant above-and-beyond action items to establish a culture of compliance and high level of reliability protection consistent with good utility practices;
8. since URE's Compliance Audit, URE has made significant improvements to its CIP compliance program. To confirm that URE's new CIP Compliance Program is performing as designed, ReliabilityFirst and URE have also agreed that ReliabilityFirst will conduct a Spot Check of URE;
9. URE volunteered to have ReliabilityFirst conduct an on-site appraisal for the management practices associated with risk management, external interdependencies, asset and configuration management, information management, implementation, integration, validation, and verification. ReliabilityFirst will evaluate and measure URE's implementation of management controls, processes, worker knowledge and skills, and technology relating to these management practices. In the event ReliabilityFirst identifies areas of improvement during the appraisal, URE will develop action plans and provide ReliabilityFirst with quarterly updates regarding the progress of these plans; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreements and supporting documentation on April 13, 2015 and approved the Settlement Agreements. In approving the Settlement Agreements, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC also considered the factors considered by ReliabilityFirst as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreements and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org	Sonia C. Mendonça* Deputy General Counsel, Vice President of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org

Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org Kristen Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0669 (216) 503-9207 facsimile kristen.senk@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Deputy General Counsel, Vice President of
Compliance and Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entities
FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3 (URE3), Unidentified Registered Entity 4 (URE4), and Unidentified Registered Entity 5 (URE5), (collectively the UREs), NERC Registry ID#s NCRXXXXX, NCRXXXXX, NCRXXXXX, NCRXXXXX, and NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty resolves two sets of violations discovered through Self-Reports and Compliance Audit findings. The violations of the Unidentified Registered Entities are the remaining open enforcement actions from a CIP Compliance Audit that the UREs contested, but ultimately agreed to mitigate. The remaining violations are Self-Reports and Compliance Audit findings, many of which are minimal risk, documentation issues that would have been eligible for Compliance Exception treatment but for UREs' relevant compliance history.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

The resolution of these violations are close in proximity to the FERC-approved settlement of 35 prior violations of the four UREs subject to this Settlement Agreement and other entities. While entering into the prior Settlement Agreement, ReliabilityFirst was aware of the extent and nature of the CIP compliance audit findings, and noted in the prior Settlement Agreement that the findings which are the subject of the instant Settlement Agreement demonstrated that UREs had made significant progress in terms of compliance. Although ReliabilityFirst was not in a position to resolve the instant Alleged Violations at that time of resolving the prior Settlement Agreement, given their isolated, mostly minimal risk nature, and the fact that they actually demonstrate a marked improvement in the UREs over time, ReliabilityFirst determined that a monetary penalty was neither necessary nor appropriate. The UREs were sanctioned fully for the shortcomings of their prior legacy CIP compliance program in the prior Settlement Agreement.

This Notice of Penalty is being filed with the Commission because ReliabilityFirst and UREs have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the UREs neither admit nor deny the violations, but have agreed to the assessed penalty of zero dollars ($0), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
RFC2012011266	CIP-002-1	R3.1	Lower/Severe	URE3; URE4; URE5	$0
RFC2012011263	CIP-002-1	R3.1	High/Severe	URE3; URE4; URE5	
RFC2012011269	CIP-002-1	R3.1	Lower/Severe	URE3; URE4; URE5	
RFC2013012717	CIP-003-3	R6	Lower/Severe	URE1	
RFC2013012401	CIP-004-3	R4	Lower/ Lower	URE1	
RFC2013012512	CIP-005-1	R1.5	Medium/ Severe	URE1	
RFC2013012402	CIP-005-3	R5	Lower/ Severe	URE1	
RFC2013013005	CIP-006-1	R1.1	Medium/ Severe	URE1; URE2	
RFC2013013006	CIP-006-1	R1.1	Medium/ Severe	URE1; URE2	
RFC2013012303	CIP-006-3c	R1.1	Medium/ Severe	URE1	
RFC2013013007	CIP-006-1	R1.8	Medium/ Severe	URE1	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
RFC2013012409	CIP-006-3c	R4	Medium/ Severe	URE1	$0
RFC2013012410	CIP-007-1	R2	Medium/ Severe	URE1; URE2	
RFC2013012413	CIP-007-1	R2	Medium/ Severe	URE1; URE2	
RFC2013012513	CIP-007-1	R3	Lower/ Severe	URE1; URE2	
RFC2013012514	CIP-007-1	R3	Lower/ Severe	URE1; URE2	
RFC2013012411	CIP-007-1	R5.2.1	Medium/ High	URE1	
RFC2013012412	CIP-007-1	R5.3.3	Medium/ Severe	URE1; URE2	
RFC2013012414	CIP-007-1	R5.3.3	Medium/ Severe	URE1; URE2	
RFC2013012753	CIP-007-3a	R1	Medium/ Severe	URE1; URE2	
RFC2013012768	CIP-007-3a	R1	Medium/ Severe	URE1; URE2	
RFC2013012718	CIP-007-3a	R6	Lower/ Severe	URE1	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-1 R3.1 (RFC2012011263, RFC2012011266, RFC2012011269)

These violations include previously unresolved, contested issues from two CIP Compliance Audits of certain URE registrations.

ReliabilityFirst conducted a Compliance Audit of URE3, URE4, and URE5. This Agreement resolves three remaining violations of CIP-002-1 R3.1 that were not resolved by the prior Settlement Agreement.

During the Compliance Audit, ReliabilityFirst discovered that URE Companies were in violation of CIP-002-1 R3.1. ReliabilityFirst discovered an electronic access control and monitoring device (EACM) that allowed Cyber Assets, specifically remote terminal units (RTUs), to connect to the EACM and communicate using a routable protocol. URE3, URE4, and URE5 failed to identify these assets as Critical Cyber Assets (CCAs).

ReliabilityFirst determined that URE3, URE4, and URE5 had violations of CIP-002-1 R3.1 because they failed to identify certain Cyber Assets essential to the operation of a Critical Asset as CCAs. The Cyber Assets, in this case the RTUs, communicated outside an Electronic Security Perimeter (ESP) using a routable protocol.

ReliabilityFirst determined the duration of the violations to be from the date URE3, URE4, and URE5 were required to comply with the Reliability Standard through when the Mitigation Plans associated with these violations are scheduled for completion.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE3, URE4, and URE5 did not identify the RTUs as CCAs, they did provide most of the protections required for CCAs, thereby reducing risk to those devices. For example, the RTUs were afforded the protections of CIP-006 and the physical access protections of CIP-004 using an advanced secure access management tool with two-factor authentication in most cases, and rigorous change control, including patching.

URE3, URE4, and URE5's Mitigation Plans to address these violations were submitted to ReliabilityFirst.

The Mitigation Plans required URE3, URE4, and URE5 to:

1. develop a new Cyber Systems Identification Methodology for Bulk Electric System (BES) assets as part of the transition to CIP Version 5 compliance, , which will require the identification of serially connected Cyber Assets associated with substations as Medium Impact BES Cyber Assets without external routable connectivity; and

2. ensure that the RTUs meet the applicable minimum requirements for Medium BES Cyber Systems.

CIP-003-3 R6 (RFC2013012717)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-003-3 R6. URE1 reported that it did not follow its change control process in one instance due to human error. URE1's change control process requires changes to be logged and approved by a member of its change management advisory committee (Committee) prior to work being executed.

Although a change was verbally approved by the supervisor of the change owner and the business unit, it was not approved by a Committee member as required. URE1 discovered the violation while reviewing change requests older than 30 days that had not been closed.

ReliabilityFirst determined that URE1 violated CIP-003-3 R6 because it failed to establish and document a process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software, and failed to implement supporting configuration management activities to identify, control, and document all entity or vendor-related changes to hardware and software components of CCAs, pursuant to its change control process.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with this Reliability Standard, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the change control process was not followed appropriately, the change was approved by knowledgeable URE1 staff prior to the start of the work. In addition, URE1 timely performed mitigating actions to prevent recurrence of the error.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. require all personnel to validate that all changes are approved and documented prior to the start of work;
2. emphasize the approval process and requirements with responsible teams during meetings in the calendar year; and
3. review the process again via email reminder in the calendar year.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (RFC2013012401)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-3 R4. URE1 reported that during a review of local users on four Physical Access Control System (PACS) servers on its corporate network, it noticed that access to the PACS was not authorized and documented through URE1's access database for certain information technology employees and contractors. Due to human error, access authorizations were not properly established for these servers. Upon discovery, URE1 removed access for the affected individuals.

ReliabilityFirst determined that URE1 violated CIP-004-3 R4 because it failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs, including the personnel's specific electronic and physical access rights to CCAs.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-004-3 R4, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the devices were not set up to ensure individuals were granted proper access through the access system, those individuals had completed CIP training and were subject to personnel risk assessment (PRAs). In addition, access was granted through an approval process with the correct asset owners, just not through the proper access database. URE1 demonstrated an otherwise strong access control program, as evidenced by a subsequent Compliance Audit identifying no additional CIP-004 issues.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. remove access for the individuals;
2. define and authorize access through the proper access database; and
3. conduct a training to communicate the new access database account configuration to relevant employees.

URE1 certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1.5 (RFC2013012512)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-1 R1.5. URE1 reported that it did not identify and document one EACM device on CIP Cyber Asset lists. Consequently, this device was not afforded all of the protections listed in CIP-005 R1.5.

URE1 conducted a root cause analysis and determined that because the EACM is not located at the Critical Asset it supports, previous routine inspections did not account for the EACM, which is located several miles from the associated Critical Asset substation. The EACM is connected via non-routable microwave transport to the substation, and this non-hard-wired connection was overlooked.

ReliabilityFirst determined that URE1 violated CIP-005-1 R1.5 because it failed to ensure that one EACM was afforded the protective measures listed in CIP-005-1 R1.5.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-005-1 R1.5, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, although the EACM is an access point to an ESP, the EACM carries non-essential data to a substation containing no CCAs. Second, the type of connectivity used by the EACM is unique within the URE1 environment, and therefore is an isolated issue. Finally, the problem was detected by URE1 and promptly mitigated upon discovery.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. bring the EACM into compliance with CIP-005 R1.5, including implementing a Physical Security Perimeter (PSP) at the associated substation; and
2. validate all electronic configurations and update documentation to reflect these changes.

URE1 certified that the above Mitigation Plan requirements were completed.

CIP-005-3 R5 (RFC2013012402)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-2 R5. URE1 reported that a new drawing became the official, active energy management system (EMS) ESP diagram, superseding a previous drawing. Subsequent to that change, four approved changes were

made to various devices related to this environment. However, the applicable ESP diagram was not updated appropriately during the 90-day requirement period.

ReliabilityFirst determined that URE1 violated CIP-005-3 R5 because they failed to update documentation within the 90-day requirement period.

ReliabilityFirst determined the duration of the violation to be from the date URE1 failed to update documentation of the ESP within 90 days of the first change, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. ReliabilityFirst determined that the issue relates solely to documentation of the changes on the ESP diagram, and appears to be an isolated incident based on the fact that no other violations of CIP-005 R5 were identified during a subsequent Compliance Audit.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. update its ESP diagram and its procedure governing how information technology CIP Cyber Asset information and lists are maintained for annual reviews and ongoing changes. URE1 placed special emphasis on the thorough verification of devices depicted on ESP diagrams;
2. validate all access points to the ESP; and
3. appropriately reflect that information with the Cyber Asset lists.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.1 (RFC2013013005 and RFC2013013006)

During the Compliance Audit, ReliabilityFirst discovered that URE1 and URE2 were in violation of CIP-006-1 R1.1.

For URE1, one facility drawing did not properly reflect the PSP, and the wiring between two PSPs was not completely enclosed by a six-wall border. For URE2, the wiring between two sets of PSPs was not contained within six-wall borders, and two rooms containing Cyber Assets were not declared as PSPs.

ReliabilityFirst determined that URE1 and URE2 violated CIP-006-1 R1.1 because they failed to ensure and document that all Cyber Assets within an ESP reside within an identified PSP.

ReliabilityFirst determined the duration of the violations to be from the date URE1 and URE2 were required to comply with CIP-006-1 R1.1, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the physical locations affected by the violations were within corporate security boundaries and therefore less likely to be subject to harm by an external malicious actor. Second, each occurrence was an isolated incident and was mitigated promptly upon discovery by URE1's and URE2's fast and thorough response. These were minor wiring, documentation, and declaration issues that were mitigated promptly before the end of the onsite audit

Prior to the conclusion of the Compliance Audit, URE1 and URE2 modified drawings, enclosed cabling in conduit, filed Technical Feasibility Exceptions (TFEs), and established PSPs where needed. ReliabilityFirst verified these mitigating activities during the Compliance Audit. In addition, URE1 and URE2 also submitted formal Mitigation Plans.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. revise the facility drawing to show that one PSP encompassed the entire floor; and
2. file a TFE to mitigate the wiring issue between the two PSPs.

URE2's Mitigation Plan required URE2 to:

1. file a TFE to mitigate the wiring issue between the two rooms containing Cyber Assets;
2. install conduit around the wiring between the two PSPs; and
3. enhance the PSP drawings to show how ESP wiring between multiple PSPs is provided physical protections.

URE1 and URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's and URE2's Mitigation Plans were complete.

CIP-006-3c R1.1 (RFC2013012303)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-3c R1.1. URE1 reported that during an inspection of a PSP during remodeling activities, URE1 discovered openings greater than 96 square inches; openings in an overhead wall, openings in PSP walls, and an opening beneath a raised floor. These non-compliant openings were not discovered previously by routine inspections conducted by an independent contractor.

ReliabilityFirst determined that URE1 violated CIP-006-3c R1.1 because it failed to document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) addressing, at a minimum, that all Cyber Assets within an ESP shall reside within an identified PSP.

ReliabilityFirst determined the duration of the violation to be from the date URE1 created the openings in the PSP, the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Access to the PSP associated with the non-compliant openings was monitored continuously by security. Additionally, of the openings discovered, an opening under the raised floor abutted against a hallway within a secured non-CIP area. Some were overhead openings that were above dropped ceilings, which resulted in very limited visibility, and could have only been accessed with a ladder. The remaining openings were in PSP walls. The wall openings were created by remodeling activities and the other wall opening abutted against a secured hallway that allowed only individuals authorized to be in the facility to enter. URE1 mitigated the issue promptly upon discovery. The discovery was a result from an internal control related to physical security.

URE1's Mitigation Plan to address this violation was submitted to ReliabilityFirst as complete.

URE1's Mitigation Plan required URE1 to:

1. perform an extent of condition review and secure all openings with steel mesh; and
2. revise its physical security plan to inspect new physical security perimeters to prevent similar violations.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (RFC2013013007)

During the Compliance Audit, ReliabilityFirst discovered that URE1 was in violation of CIP-006-1 R2.2. URE1 used two terminal servers as workstations for its PACS, but did not identify those terminal servers as a PACS system, therefore failing to provide some of the protections identified in CIP-006 R2.

ReliabilityFirst determined that URE1 violated CIP-006-1 R1.8 because it failed to document and implement the operational and procedural controls to manage physical access at two access points to the PSPs twenty-four hours a day, seven days a week with one or more physical access methods.

ReliabilityFirst determined the duration of the violation to be from the date URE1 was required to comply with CIP-006-1 R1.8, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The terminal servers cannot be used to authorize or log access directly to PSPs. The terminal servers themselves are located in PSPs and were afforded most of the protections required by CIP-006 R1.8. In addition, prior to the Compliance Audit, URE1did not realize these terminal servers could be considered part of the PACS system and should therefore be subject to the protections listed in CIP-006 R1.8. Thus, the violation did not result from a failure to institute internal controls for physical security.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst. The Mitigation Plan required URE1 to ensure the two terminal servers meet all CIP Standard requirements.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-006-3c R4 (RFC2013012409)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-3c R4. URE1 reported that an employee without authorized unescorted access to a substation accessed the substation without a valid key card. When the entry was made, URE1's security alarms station received an alarm, security technicians immediately investigated and escorted the employee out of the substation.

A physical security technician determined that the door lock had been disabled for the substation door and the actuation of a push button lever inside the door locking mechanism allowed the employee to

enter the substation. Although URE1 cannot conclusively determine the duration of the condition, it believes the period to be less than five days. A locksmith permanently disabled the levers in the substation door-locking mechanisms.

ReliabilityFirst determined that URE1 violated CIP-006-3c R4 because it failed to document and implement the operational and procedural controls to manage physical access at all access points to the PSP twenty-four hours a day, seven days a week with one or more physical access methods.

ReliabilityFirst determined the duration of the violation to be from the earliest date that URE1 believes it did not manage the physical access point, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The door was adequately monitored during the period the lock was mechanically disabled. Only one unauthorized entry occurred during this period. The unauthorized individual was an employee with a current PRA. His entry to the substation was observed by authorized employees. The entry also resulted in an alarm, and security personnel ensured the individual was escorted out of the substation within ten minutes of his entry. In addition, the substation is located within a protected area that is continuously staffed with security officers.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. contract a locksmith to replace the locking mechanism with a proper lock;
2. perform an evaluation to determine if any additional inadequate lock mechanisms were installed at other substation PSPs; and
3. replace three additional inadequate locking mechanisms, which were identified through the extent-of-condition evaluation.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

<u>CIP-007-1 R2 (RFC2013012410 and RFC2013012413)</u>

URE1 and URE2 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R2. URE1 and URE2 reported that their Cyber Vulnerability Assessments (CVAs) were the first under the new CIP compliance program.

The CVAs used a new procedure that provides better visibility to ports and services and demonstrated that existing documentation of ports and services was inadequate. URE1 identified Cyber Assets for which ports and services not needed for normal or emergency operations were not disabled, and Cyber Assets for which ports or services were not documented correctly. URE2 identified Cyber Assets for which ports and services not needed for normal or emergency operations were not disabled, and Cyber Assets for which ports or services were not documented correctly.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R2 by failing to implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.

ReliabilityFirst determined the duration of the violations to be from the date URE1 and URE2 were required to comply with CIP-007-1 R2, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a moderate and not serious or substantial risk to the reliability of the BPS. A significant number of Cyber Assets suffered the deficiency, which potentially created vulnerabilities on those Cyber Assets for an extended period. Layers of defense on the UREs' network, such as intrusion prevention, limit the risk and exposure of devices to external threats. URE had robust intrusion prevention appliances on the internet-facing side of its environment and has intrusion prevention services on its firewalls in front of its EMS/GMS ESPs. URE1 and URE2 mitigated these violations by self-identifying the issues through improvements to its post-merger compliance program and performing thorough mitigation.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. perform an evaluation of the ports and services program and procedures;
2. revise the associated procedures to improve the effectiveness, efficiency, and documentation of the CIP-007 R2 configuration program and shift the performance of CIP-007 R2 activities to asset owners and administrators; and
3. add new controls that track all changes made to the documentation. The controls relate back to the ticket that was generated in the change control and configuration management system.

URE1 and URE2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-1 R3 (RFC2013012513 and RFC2013012514)

URE1 and URE2 submitted identical Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R3. URE1 and URE2 reported that during a system account review of the CIP environment they did not meet the 30-day self-imposed time limit in their security patch management program for documenting a patching implementation plan on two CCAs (servers).

Soon after the discovery of the violations, URE1 and URE2 developed an implementation plan to retire the two servers and migrate associated guest servers to physical servers, with all patches applied.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R3 because they failed to provide sufficient evidence that their security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for Cyber Assets within the ESP was implemented for two applicable assets.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable for URE1 and URE2, through the date URE1 and URE2 completed their respective Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the violations affected only two devices and were caused by an isolated human error, and there were no indications of a systemic failure in assessing or implementing security patches. Second, although the self-imposed 30-day time limit for patch implementation plan documentation was not met, applicable security patches and security upgrades were assessed for applicability within 30 calendar days as specifically required by the Standard. Finally, the subsequent Compliance Audit revealed no further violations of CIP-007 R3.

URE1's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

URE2's Mitigation Plan to address its violation was submitted to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. develop and review an implementation plan and retire the Cyber Assets affected; and

2. develop an internal control mechanism to monitor whether business units and/or system administrators document patch implementation plans within 30 days from the date of notification by their internal cyber security department.

URE1 and URE2 certified that the above Mitigation Plans' requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-1 R5.2.1 (RFC2013012411)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-1 R5.2.1. URE1 reported that due to misleading documentation, URE1 failed to rename several EACM accounts as required by CIP-007 R5.2.1. In addition, URE1 reported that it failed to rename one other local default administrator account. These issues were discovered when a new tool for password change review was implemented. The violation affected Cyber Assets.

ReliabilityFirst determined that URE1 violated CIP-007-1 R5.2.1 because they failed to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts, including the removal, disabling, or renaming of such accounts where possible.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE1, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the risk was mitigated partially by the Cyber Assets' location behind firewalls in an ESP; separate user accounts are required to log into the network, which were subject to multiple password change cycles. Second, although the accounts were not renamed for a long period and several cycles of CVAs did not identify the issue, URE1 has since significantly improved these internal controls, which enabled it to identify and self-report the issue.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. develop and implement a plan utilizing URE1's Change Management Process to rename the local administrator account on all affected devices;

2. rename the single account and a new step was added to the CIP server build process;
3. develop an improved CVA program that is capable of promptly identifying these types of deficiencies; and
4. perform an annual review of CIP Cyber Asset passwords and accounts. As part of these reviews, administrator, shared, and other generic accounts are reviewed to ensure they are still valid and required.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

CIP-007-1 R5.3.3 (RFC2013012412 and RFC2013012414)

URE1 and URE2 submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-1 R5.3.3. URE1 reported that the passwords on local server accounts were not changed annually, and URE2 reported that the passwords on additional local server accounts were not changed annually. In both cases, although URE1 and URE2 have a procedure for annual local administrator account password updates, they missed the affected accounts because they were not documented in the password vault used to manually manage passwords. These password deficiencies were identified shortly after URE1 and URE2 implemented a new tool for password change reviews.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-1 R5.3.3 because they failed to require and use passwords that are changed at least annually.

ReliabilityFirst determined the duration of the violations to be from the date URE1 was required to comply with CIP-007-1 R5.3.3, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the affected Cyber Assets are located behind firewalls in an ESP, and separate user accounts are required to log into the network, which were subject to multiple password change cycles through the duration of the violation. Second, although the passwords were not changed for a long period and several cycles of CVAs did not identify the issue, URE1 and URE2 have since significantly improved these internal controls, which enabled them to identify and self-report the issue.

URE1's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst.

The Mitigation Plans required URE1 and URE2 to:

1. create a report that validates password changes and documents the use of the report in the associated procedure; and
2. add a new step to the CIP server build process to perform a peer review of the local server accounts for the new server and verify that the accounts and passwords are documented.

URE1 certified that the above Mitigation Plan requirements were completed. UER2 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

ReliabilityFirst verified that URE2's Mitigation Plan was complete.

CIP-007-3a R1 (RFC2013012753 and RFC2013012768)

URE1 and URE2 each submitted Self-Reports to ReliabilityFirst stating that they were in violation of CIP-007-3a R1. URE1 and URE2 did not maintain complete documentation of test results for significant changes on CIP Cyber Assets. URE1 did not document significant changes on Cyber Assets, and URE2 did not document significant changes on additional Cyber Assets.

ReliabilityFirst determined that URE1 and URE2 violated CIP-007-3a R1 because they failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls and failed to document test results.

ReliabilityFirst determined the duration of the violations to be from the date URE2 first failed to comply with CIP-007-3a R1, through the date URE1 and URE2 completed their Mitigation Plans.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the violations were primarily a documentation issue, since URE1 and URE2 performed appropriate testing. Second, although not complete enough to meet the threshold of compliance, URE1 and URE2 did document some testing. Finally, URE1's and URE2's follow-up testing verified there were no adverse effects on the production system from the testing documentation inadequacies.

URE1's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst. URE2's Mitigation Plan to address its violation was submitted as complete to ReliabilityFirst.

URE1's and URE2's Mitigation Plans required URE1 and URE2 to:

1. have follow-up testing to verify that no adverse effects on the production systems or the operation of the production systems resulted from the testing documentation inadequacies;
2. meet with personnel to review and reinforce requirements and expectations for documenting test results for significant changes to CIP Cyber Assets; and
3. provide refresher training sessions to review and reinforce requirements and expectations of test results documentation for appropriate personnel.

URE1 and URE2 certified that the above Mitigation Plans' requirements were completed.

ReliabilityFirst verified that the Mitigation Plans were complete.

CIP-007-3a R6 (RFC2013012718)

URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R6. URE1 reported that logs of system events over a 25-day period for one CCA were not retained for the full 90 days, as required by CIP 007-3a R6.

ReliabilityFirst determined that URE1 violated CIP-007-3a R6 because it failed to ensure that a Cyber Asset within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

ReliabilityFirst determined the duration of the violation to be from the date the CCA was initially misconfigured, through the date URE1 completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the log entries were missing for one CCA device, this CCA device exists within the ESP, behind firewalls. The process and procedures were in place to monitor and log access at access points in the ESP. However, the violation was discovered by an effective internal control (quarterly review) and was limited to one device for a 25-day period before URE1 correctly configured it. In addition, no additional violations of CIP-007 R6 were discovered at the subsequent Compliance Audit.

URE1's Mitigation Plan to address this violation was submitted as complete to ReliabilityFirst.

URE1's Mitigation Plan required URE1 to:

1. update a CIP server build procedure to emphasize the step for configuring the CCA to back up logs and automate alerting for potential cyber security failed login attempts;
2. add a CIP server build procedure for the peer review process; and
3. add a procedure step to include additional signoffs confirming that a test of the log backup configuration and automated alerting was successful.

URE1 certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE1's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed no monetary penalty for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. The UREs had prior violations of the subject NERC Reliability Standards. ReliabilityFirst did not consider these prior violations as aggravating factors in the penalty determination because the prior instances were isolated incidents that did not indicate repetitive conduct or systemic issues;
2. The UREs had an internal compliance program at the time of the violations which ReliabilityFirst considered a mitigating factor;
3. ReliabilityFirst determined that the UREs had made significant progress in terms of compliance since the Compliance Audit, which was considered a mitigating factor in the penalty determination.
4. The UREs self-reported 11 of the violations;
5. The UREs were cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. The violations of RFC2013012410 and RFC2013012413 posed a moderate but did not pose a serious or substantial risk to the reliability of the BPS while the rest of the violations posed a minimal risk, as discussed above; and
8. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that no penalty is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 13, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	Sonia C. Mendonça* Deputy General Counsel and Vice President of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Kristina Pacovsky* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0670 (216) 503-9207 facsimile kristina.pacovksy@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org Niki Schaefer* Managing Enforcement Attorney ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile niki.schaefer@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Deputy General Counsel and Vice President
of Compliance and Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entities
ReliabilityFirst

Attachments

August 31, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations discussed in detail in the Settlement Agreement, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE stipulates to the facts in the Settlement Agreement, admits that those facts constitute violations, and has agreed to a monetary penalty of four

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

hundred twenty-five thousand dollars ($425,000) and a non-monetary sanction of a Spot Check, in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement and below.

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2013013255	CIP-002-3	R2	High/ High	SR	$425,000
RFC2013013256					
RFC2014014057	CIP-002-3	R3	High/ High	CA	
RFC2014014058					
RFC2014014059					
RFC2014014034	CIP-003-3	R2.3	Medium/ High		
RFC2014014035					
RFC2014014036					
RFC2014014031	CIP-003-3	R4	Medium/ Severe		
RFC2014014032					
RFC2014014033					
RFC2014014028	CIP-003-3	R5.2	Lower/ Severe		
RFC2014014029					
RFC2014014030					

[4] Violation Risk Factor (VRF) and Violation Severity Level (VSL)

[5] Self-Report (SR) / Self-Certification (SC) / Compliance Audit (CA) / Spot Check (SPC) / Compliance Investigation (CI).

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2013012765	CIP-003-3	R6	Lower/ Severe	SR	
RFC2014013308	CIP-003-1	R6	Lower/ Severe	SR	$425,000
RFC2014013311					
RFC2014013314					
RFC2014013710	CIP-004-3a	R2	Medium/ Severe		
RFC2014013714	CIP-004-3a	R4	Lower/ Lower		
RFC2014013693			Lower/ Severe		
RFC2014013695					
RFC2014014025	CIP-005-3a	R1.4, R1.6	Medium/ Severe	CA	
RFC2014014026					
RFC2014014027					
RFC2014014054	CIP-005-3a	R2.1, R2.2, R2.4	Medium/ Severe		
RFC2014014055					
RFC2014014056					
RFC2014013312	CIP-005-3a	R2.2	Medium/ Severe	SR	
RFC2014013332					
RFC2014013367					
RFC2014014169	CIP-005-1	R4	Medium/ Severe		
RFC2014014170					
RFC2014014171					
RFC2014014051	CIP-005-3a	R5.1	Lower/ High	CA	
RFC2014014052					
RFC2014014053					
RFC2014013309	CIP-006-3c	R1.1	Medium/ Severe	SR	
RFC2014014048	CIP-006-3c	R1.1	Medium/ Severe	CA	
RFC2014014049					
RFC2014014050					
RFC2014014040	CIP-006-3c	R1.1	Medium/ Severe		
RFC2014014041					
RFC2014014042					
RFC2014013320	CIP-006-3c	R1.6	Medium/ Severe	SR	
RFC2014013326					
RFC2014013333					

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2014014044	CIP-006-3c	R1.6.1	Medium/ Severe	CA	
RFC2014014046					
RFC2014014047					
RFC2014014037	CIP-006-3c	R2.2	Medium/ Severe	CA	$425,000
RFC2014014038					
RFC2014014039					
RFC2015014591	CIP-006-3c	R5	Medium/ Severe	SR	
RFC2014013322	CIP-007-3a	R1.3	Lower/ Severe		
RFC2014013327					
RFC2014013334					
RFC2014013335	CIP-007-3a	R2	Medium/ Severe		
RFC2014014072	CIP-007-3a	R2.1, R2.2	Medium/ Severe	CA	
RFC2014014073					
RFC2014014074					
RFC2013012767	CIP-007-3a	R2.2	Medium/ Severe	SR	
RFC2014013310	CIP-007-1	R2.2	Medium/ Severe		
RFC2014013313					
RFC2014013315					
RFC2014013321	CIP-007-3a	R3.1	Lower/ Severe		
RFC2014013328					
RFC2014013336					
RFC2014014078	CIP-007-3a	R3.1, R3.2	Lower/ Severe	CA	
RFC2014014079					
RFC2014014080					
RFC2014013692	CIP-007-1	R4	Medium/ Severe	SR	
RFC2014013694					
RFC2014013696					
RFC2014014069	CIP-007-3a	R4.1, R4.2	Medium/ Severe	CA	
RFC2014014070					
RFC2014014071					
RFC2014014066	CIP-007-3a	R5.1.2, R5.2, R5.2.1,	Medium/ Severe		
RFC2014014067					

NERC Violation ID	Standard	Req	VRF/ VSL[4]	Discovery Method[5] Date	Penalty Amount
RFC2014014068		R5.2.2, R5.2.3			
RFC2014013428	CIP-007-3a	R5.2, R5.3	Lower/ Severe	SR	
RFC2014014009	CIP-007-3a	R5			
RFC2014013323	CIP-007-3a	R5.1.1, R5.1.3	Lower/ Severe	SR	
RFC2014013329					
RFC2014014008					
RFC2014014063	CIP-007-3a	R6.1, R6.4	Medium/ Severe	CA	
RFC2014014064					
RFC2014014065					
RFC2014013324	CIP-007-1	R6.5	Lower/ Severe	SR	
RFC2014013330					
RFC2014013338					
RFC2014014060	CIP-007-1	R8.2, R8.3	Medium/ Severe	CA	
RFC2014014061					
RFC2014014062					
RFC2014013325	CIP-007-3a	R8	Medium/ Severe	SR	
RFC2014013331					
RFC2014013339					
RFC2014014075	CIP-008-3	R1.6	Lower/ High	CA	
RFC2014014076					
RFC2014014077					
RFC2014013378	CIP-009-3	R5	Lower/ Severe	SR	
RFC2014013379					

$425,000

OVERVIEW

The Settlement Agreement resolves 102 violations of CIP Reliability Standards.

ReliabilityFirst determined there were several overarching factors that contributed to the violations, including inconsistent processes and procedures across URE functional groups, charging its Information Technology Department (the IT Department) with primary responsibility for CIP compliance, and manual processes that were ineffective and more susceptible to error. URE identified these overarching factors prior to its Compliance Audit and immediately engaged ReliabilityFirst to develop a plan to address them.

URE implemented systematic changes (such as overhauling numerous procedures and adding automation tools) to enhance CIP compliance culture and increase their preparedness for the CIP Version 5 Requirements which become effective on April 1, 2016. To address the underlying root causes of the violations, URE, among other things: 1) moved the CIP compliance function from the IT Department to a different department to help implement and oversee consistent processes; 2) consolidated its CIP policies and procedures–resulting in a 75% reduction in documents used for implementing CIP-related controls; and 3) automated processes where practicable. Through mitigation and above-and-beyond activities, URE increased its maturity in the core management practices of reliability quality management, workforce management, information management, and asset and configuration management. In addition to the strengthening of its compliance functions and subject matter expertise, URE also increased its capacity in the Human Resources Department to support the training of personnel on CIP compliance responsibilities.

CIP-002-3 R2 (RFC2013013255)

ReliabilityFirst determined that URE failed to complete the annual Critical Asset identification process within the required timeframe. Due to an oversight finalizing supporting documentation, the process was delayed by approximately two months.

ReliabilityFirst determined the duration of the violation to be from when URE should have added a substation to its list of Critical Assets, through when URE updated its Critical Asset and Cyber Asset list.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The substation was on URE's Critical Cyber Asset (CCA) list. In addition, the substation in question was at all times being protected as part of URE's Critical Assets and CIP program. Finally, the duration of the violation was relatively short.

URE's Mitigation Plan (RFCMIT010275) to address this violation was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. revise and update its Critical Asset and Cyber Asset lists; and
2. revise its Critical Asset and CCA identification procedures.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-002-3 R2 (RFC2013013256)

ReliabilityFirst determined that URE failed to complete the annual Critical Asset identification process within the required timeframe. Due to an oversight finalizing supporting documentation, the process was delayed by approximately two months. During the review, the responsible individual identified a change from the initial results in that substations not previously on the Critical Asset list were required to be added to the Critical Asset list.

ReliabilityFirst determined the duration of the violation to be from when URE should have added the substations to its Critical Asset list, through when URE updated its Critical Asset and Cyber Asset list.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had treated the substations at issue as essential assets for several years prior to the violation and they had CIP protections. In addition, the locations have had physical asset controls in place for several years along with electronic access controls to promote the security and reliability of the BPS. Finally, the duration of the violation was relatively short.

URE's Mitigation Plan (RFCMIT010276) to address this violation was submitted to ReliabilityFirst as complete.

The URE Mitigation Plan required URE to:

1. revise and update its Critical Asset and Cyber Asset lists; and
2. revise its Critical Asset and CCA identification procedures.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-002-3 R3 (RFC2014014057, RFC2014014058, and RFC2014014059)

ReliabilityFirst determined that URE failed to develop its lists of CCAs using the lists of Critical Assets developed pursuant to CIP-002-3 R2. The failure related to a relay and Supervisory Control and Data Acquisition (SCADA) Protocol Translator (SPT) terminal servers. The instances of failure were due to the lack of training for the individuals installing Cyber Assets, who failed to follow processes, and a lack of effective asset and configuration management controls. In addition, URE did not have a procedure for adding, removing, or modifying Cyber Assets into the URE CIP environment.

ReliabilityFirst determined the duration of the violations began when URE published a CCA list without the CCA at issue and CCAs were placed into production, through when URE published a corrected CCA list.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not developing a complete lists of CCAs increased the risk that URE would miss CCAs that were not on the list when implementing the security controls.

The relay was tested prior to implementation and was afforded all of the required security protections and standards for CCAs. Based on the CCA list, there were SPT terminal servers that were re-commissioned and not accounted for on the CCA list. However, the devices did not have external communication capabilities as they were only configured to communicate within the ESP, but not accounted for on the CCA list and not afforded cyber security controls as required by the CIP standards.

URE's Mitigation Plan (RFCMIT011116-1) to address these violations was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. complete the commissioning process for the relay and SPT terminal server Cyber Assets and audit the results;
2. review URE processes for the definition of significant change and determine if that covers potential conditions related to the CIP environment. This included how a change in one part of the CIP environment needs to be considered in other parts of the CIP environment;
3. review potential modifications to the URE CIP commissioning and change and configuration management processes for additional refinements with URE personnel who would start the change management process, review and approve the change request, and then execute the changes to the CIP environment;
4. review asset management processes and data to determine if the appropriate Cyber Asset data is maintained over the life-cycle of the Cyber Asset. This would include information on initial purchase, configuration, deployment, modifications, re-deployment, and disposal;
5. interview Subject Matter Experts (SMEs) involved in Cyber Asset commissioning to determine areas of confusion that create inconsistent compliance application and results;
6. review URE processes and tools to remove any potential confusion on execution and capture the recommendations;

7. establish asset management processes and database for all URE functional departments involved with the CIP environment;
8. update or create URE process(es) per the recommended modifications. This will include determination of internal controls to assist in the prevention and detection of conditions which would lead to non-compliance;
9. conduct training for all URE personnel, that work in or affect the CIP environment on the revised and new processes and controls; and
10. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003-3 R2.3 (RFC2014014034, RFC2014014035, RFC2014014036)

ReliabilityFirst determined that URE failed to have the CIP senior manager or a designee approve delegations. The violations were due to a lack of effective workforce management controls in not training personnel on the requirement to have the CIP senior manager or designee sign the policies at issue.

ReliabilityFirst determined the duration of the violations to be from when the first document was published without the necessary signature, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the CIP senior manager designee was not a signatory to the policy identifying the delegations, an executive, who is involved in URE's compliance program, did review and approve the policy. Senior management had visibility into compliance matters and specifically approved certain delegations, minimizing the possibility of security actions outside of defined and approved processes.

The URE Mitigation Plan (RFCMIT011257) to address these violations was submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. revise and release a revision of the relevant document signed by the CIP senior manager designate. In addition, URE removed all delegations previously included, except for an emergency successor;

2. host a series of sessions to develop strategies to remediate delegation and designation of the CIP senior manager and associated duties. These sessions involved the CIP-003 Standard owner, director of CIP initiatives, URE information officer and NERC CIP senior manager, along with a third-party compliance consultant;
3. revise the relevant document to only cover the name, title, date of designation, and responsibilities for the assigned CIP senior manager designate;
4. establish and implement a policy document for when the CIP senior manager designate assigns authority to a delegate, or delegates. This new policy document will cover the why, when, and how the CIP senior manager designate will delegate specific authority to a delegate or delegates;
5. distribute informational communication to URE management with distribution of new policy for when the CIP senior manager designate assigns authority to a delegate or delegates. The policy describing the delegation of authority by the CIP senior manager designate will go to the URE management staff that will be on the distribution list for when delegations occur;
6. set-up an electronic distribution list for the CIP senior manager designate to use for distribution of a standardized email communication notifying appropriate URE management of situations in which authority has been delegated for specific actions to named delegate or delegates, for a discrete period of time. The email communication will include the named delegate, or delegates, their titles, contact information, discrete period of time, and the specific actions in which they have been delegated authority; and
7. set up a secure folder with access limited to specific personnel for the storage of the email communications from the CIP senior manager designate.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003-3 R4 (RFC2014014031, RFC2014014032, RFC2014014033)

ReliabilityFirst determined that URE failed to identify, classify, and protect CCA information that resided on third-party hardware. URE failed to consider the protection of CCA information in dealing with the third-party vendor and the contract did not include access provisions or stipulations for how CCA information would be protected.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because URE did not have controls in place to ensure that the third-party vendor was protecting their CCA information housed by the third-party vendor, including internet connection sharing (ICS) devices, names, user IDs, and passwords, which could have exposed the CCA information to unauthorized access. Although information protection was not explicitly documented in the third-party contract, the vendor in question has a high-level of exposure with the CIP requirements, is aware of the necessity to protect URE CCA information, and has a good reputation for maintaining security.

URE's Mitigation Plan (RFCMIT011117-1) to address these violations was submitted to Reliability First.

URE's Mitigation Plan required URE to:

1. create a document requiring information management and protection controls;
2. develop an information management and protection business assessment strategy for all systems, internal and external;
3. revise its information protection program to address protection of CIP information on third-party systems;
4. implement an information management and protection business assessment strategy for all systems, internal and external;
5. complete the execution plan based on the outcome of the information management and protection business assessment of the systems;
6. assess existing CIP environment URE vendor contracts to determine if the appropriate level of information management and protection exists based on the revised and newly created controls;
7. revise existing contract to include information management and protection controls as required by revised URE policies;
8. develop a corporate policy for information management and vendor contract language; and procedure for identifying contracts that require critical energy infrastructure information (CEII) protections and non-disclosure agreements (NDAs);
9. provide training on revised or newly developed information protection plan, policies and procedures;

10. implement a corporate policy for information management and vendor contract language; and procedure for identifying contracts that require CEII protections and NDAs; and
11. perform verification that applicable CIP environment vendors are adhering to the contractual obligations.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003-3 R5 (RFC2014014028, RFC2014014029, RFC2014014030)

ReliabilityFirst determined that URE failed to conduct an annual review of access privileges to protected information, specifically the privileges assigned to access roles in URE's access request and approval system. URE did not have a defined policy or methodology for managing privileges assigned to roles due to the complexity and magnitude of the CIP program outgrowing URE's resources and access management practices.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not having a thorough annual review including verifying privileges in URE access request and approval system versus actual privileges on devices increased the risk of inadvertent unauthorized access to CCA information. In addition, not maintaining a list of personnel authorizing access to the CCA information areas increased the possibility of granting unauthorized access without the proper approvals. However, URE did review the access lists quarterly, updates, and maintains access in accordance with the results of those reviews. Also, URE had other safeguards in place to protect against unauthorized access to CCA information, such as cameras at the Physical Security Perimeters (PSPs) monitoring access logs.

URE's Mitigation Plan (RFCMIT011258) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. establish business processes to execute and document a complete review and management of URE personnel accesses for all functional groups;
2. perform and document an assessment and evaluation of administrative, technical, and procedural controls of access privileges;

3. create or revise existing processes and methodologies for access control based on the assessment and evaluation results;
4. develop a management process for enterprise-wide job role privilege provisioning and revocation;
5. refine the annual review process to incorporate enterprise roles and all associated access privileges;
6. execute the refined annual review process to review access privileges; and
7. configure the technical tools in place to enhance capturing user and role access, reporting features, and automate review process.

URE certified that the above Mitigation Plan requirements were completed.

CIP-003 R6 (RFC2013012765)

ReliabilityFirst determined that URE failed to publish specific configuration procedures and failed to follow its change control and configuration management process for CIP baseline testing and implementation of interface cards. URE discovered this violation during its Cyber Vulnerability Assessment (CVA).

ReliabilityFirst determined the duration of the violation to be from when URE commissioned and placed the interface cards into service, through when URE disabled the applicable ports.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices at issue were non-CCAs inside the Electronic Security Perimeter (ESP) and PSP that only provide an Ethernet-to-serial protocol conversion to allow communication. The protective measures for the ESP, such as the firewall rules and security event monitoring, and the PSP, such as the card access and video monitoring, reduced the risk posed by the non-CCA devices.

URE's Mitigation Plan (RFCMIT010170) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. create IP ports and services procedure for interface cards; and
2. disable the IP ports for the cards.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-003 R6 (RFC2014013308, RFC2014013311, RFC2014013314)

ReliabilityFirst determined that URE failed to publish configuration procedures and failed to follow URE change control and configuration management process. Specifically, URE discovered during its CVA that it had enabled unnecessary IP ports on certain Physical Access Control Systems (PACS) due to not changing a factory setting enabling ports not necessary for normal operation.

ReliabilityFirst determined the duration of the violations to be from when URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices at issue were non-CCAs inside the ESP and PSP that only provide an Ethernet-to-serial protocol conversion to allow communication. The protective measures of the ESP, such as the firewall rules and security event monitoring, and the PSP, such as the card access and video monitoring, reduced the risk posed by open ports on these non-CCA devices.

URE's Mitigation Plan (RFCMIT011288) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. review and revise the master security configuration to ensure the ports are properly documented;
2. establish a change and configuration committee to align URE functional groups and build commitment, manage CIP environment changes, and enable URE to support the complex process of implementing configuration changes that may affect various functional groups. Establishing and achieving change management objectives helps URE more effectively implement the changes necessary to maintain operations and adhere to compliance requirements. This committee will serve as a formal peer-to-peer information sharing and support forum.
3. revise current URE processes and procedures to include procurement, risk assessment, asset management, supply chain, and testing trigger points, requirements, and hand-offs;
4. conduct training for all URE personnel that work in or affect the CIP environment on the resulting revised and new processes and controls;

5. perform an assessment of current URE software and tools used by all functional groups for change management and configuration controls to determine if there is a single tool or combination of limited tools that can be leveraged and implement accordingly to support URE's CIP compliance program thereby mitigating the number of existing tools URE employs to support change and configuration management; and
6. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-004-3a R2 (RFC2014013710)

ReliabilityFirst determined that URE failed to ensure that all personnel having access to CCAs were trained prior to being granted such access. URE discovered that certain joint operating company (JOC) personnel had not completed the mandatory annual JOC CIP training. URE notified its corporate security department, which deactivated access cards for the identified personnel. The discrepancies were due to an inaccurate tracking report that had an incorrect field, resulting in URE not reviewing or verifying certain criteria. This in turn was due to ineffective verification and workforce management controls, such as training.

ReliabilityFirst determined the duration of the violation to be from the date when the annual training for the first individual was due to be completed, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failing to ensure personnel are trained prior to access increases the likelihood that untrained personnel may have cyber or unescorted physical access to CCAs. However, the individuals URE identified for failing to complete the mandatory annual training did timely complete previous training and there were no material changes from the previous training to the missed training. In addition, URE immediately revoked access upon identifying the individuals who did not complete training, and reinstated the access after the individuals completed the appropriate training.

URE's Mitigation Plan (RFCMIT011268) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. reprimand the administrator responsible for the training system during the time of the described occurrence, make them aware of the issue, and reinforce the training requirements of Standard CIP-004;
2. hire a dedicated resource to centralize the management of the learning management system (LMS). This resource would be responsible for enrollment, tracking, and validating completion of appropriate training, generating and distributing reports, and other duties as required;
3. populate appropriate fields in LMS after performing a manual validation and reconciliation process to determine the extent of conditions, resulting in the creation of a list of active JOC personnel required to take the mandatory annual JOC training;
4. correct the LMS reporting procedure to provide consistent LMS reporting information based on the same criteria used for training enrollment;
5. establish a training enrollment process and procedure for required URE training modules;
6. establish a periodic reporting process to identify when there are [EMPTY or BLANK] fields in LMS user training records; and
7. establish a data integrity auditing process for the LMS user training records.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

CIP-004-3a R4 (RFC2014013714)

ReliabilityFirst determined that URE failed to revoke access to CCAs within seven calendar days for personnel who no longer require such access to CCAs. A URE JOC identified instances involving individuals who retired without the URE JOC collecting their access badges or informing URE to remove their access. The URE JOC also identified an instance in which it had delayed informing URE to terminate a contractor's physical access to a CIP facility. The failures were due to a lack of effective workforce management controls and training.

ReliabilityFirst determined the duration of the instances to be from the dates URE was required to remove access through the dates it removed access.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, not revoking authorized access upon retirement permits unauthorized access to

CCAs, which could put the BPS at risk. The individuals no longer required access, but URE did not take their access badges upon retirement. Thus, those individuals or anyone who may have had access to those badges could have accessed the CCAs located at critical facilities. Although the employees were trusted employees who completed all of the requirements and training to be granted physical access to CCAs, there was the potential for this same violation to have occurred with other individuals, such as contractors, because of process gaps relating to notice to URE of individuals who no longer require access. In addition, at least for the first instance, it took over two months to notify URE of the first employee's retirement, and discovery only occurred as the result of a quarterly review. Finally, all these instances indicate a programmatic failure related to CIP-004 R4 with similar violations occurring over a three-year period.

URE's Mitigation Plan (RFCMIT011282) to address this violation and violation IDs RFC2014013693 and RFC2014013695, discussed in more detail below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. develop active directory plan for URE's access management system;
2. conduct internal review of JOC access management to develop/revise process to document job role, job function, and business "need-to-know";
3. conduct access management shareholder meeting to review/identify other automated systems for integration into URE's access management system and identify systems that are technically unable to integrate;
4. develop and execute interim process to routinely reconcile URE's access management system approved access to active directory provisioned access;
5. develop integration plan for identified access management systems;
6. develop business process to manage CIP and Non-CIP roles as they are added to URE's access management system to include "need-to-know" business case;
7. engage JOCs to conduct a thorough review of personnel with unescorted physical access and logical access to URE assets, and establish guidelines to implement reviews and increase frequency of reviews;
8. review and revise its procedure to integrate the business process;
9. perform and document an assessment of the current active directory security groups to identify/validate access controllers;

10. complete URE's access management system integration for identified systems;
11. complete update of all active directory security groups and ensure group members have appropriate "need-to-know";
12. configure and enable the URE's access management system reconciliation report to identify discrepancies in access privileges;
13. refine the annual and quarterly review processes to incorporate new business process;
14. establish and implement internal controls for recognition of process execution failures; and
15. conduct training for all URE personnel that work with or affect the access management process resulting from the revised/new processes and controls.

URE certified that the above Mitigation Plan requirements were completed.

CIP-004-3a R4 (RFC2014013693, RFC2014013695)

ReliabilityFirst determined that URE failed to maintain access lists of employees with access to CCAs properly. URE's access management system was unable to demonstrate specific access requests and revocations of sampled personnel with access to IT services within the audit timeframe. This failure was due to ineffective verification controls and insufficient training.

ReliabilityFirst determined the duration of the violation to be from the date URE failed to maintain a list of personnel with authorized cyber or authorized unescorted physical access to CCAs, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because not having an accurate record of access privileges increases the risk of inadvertent unauthorized access to CCA Information. However, although access was not properly recorded, URE confirmed that actual access was maintained and removed as intended for all affected employees and the employees had completed all requirements to be granted access to CCAs.

URE's Mitigation Plan (RFCMIT011282) to address these violations is described in RFC2014013714 above.

CIP-005-3a R1.4, R1.6 (RFC2014014025, RFC2014014026, RFC2014014027)

ReliabilityFirst determined that URE failed to identify certain non-CCAs at URE's control centers within the respective ESPs and failed to identify all ESP access points at URE's control centers. The violation affected Cyber Assets that are used to provide GPS data to establish time values, and redundant firewall Cyber Assets. At the time URE deployed the assets, URE personnel did not understand that all Cyber Assets residing within an ESP must be identified as either a CCA, Electronic Access Control and Monitoring device (EACM), PACS, or Protection Cyber Asset (PCA) even if the Cyber Asset is not directly connected to the ESP internal network.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous URE CIP Compliance Audit, through the date URE updated its documentation to include the GPS data Cyber Assets in the Cyber Asset lists for both control centers.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. First, URE does not consider the GPS data Cyber Assets as essential to the operation of the control center. Second, the GPS data Cyber Assets resided within an ESP and PSP and are not directly accessible from the internet, but rather only locally accessible, and thus were protected from unauthorized access. Third, URE did document the primary firewall physical and logical ports as access points because the primary and secondary firewalls are logically considered as a single Cyber Asset with a single management interface and configuration. Finally, the devices are housed in an identified PSP, which allows only authorized physical access.

URE's Mitigation Plan (RFCMIT011267) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update the Cyber Asset list to indicate GPS data Cyber Assets within the ESP, and to include the secondary firewall as an Access Point;
2. review URE processes for the definition of "significant change" and determine if it covers all potential conditions related to the CIP environment. This would include when a Cyber Asset is introduced to the CIP environment, how should it be classified if there is redundant hardware or if it is not directly connected to an ESP network, but to Cyber Assets within the ESP, and the overall effect to the CIP environment of those connections;
3. interview and survey SMEs involved in Cyber Asset commissioning to:
    a. assess their understanding of what is a "significant change";

b. determine what is required for a "significant change"; and

c. suggest methods to improve processes on identification of "significant change" and how they should be processed.

4. determine how to take into account redundant hardware Cyber Assets and how they should be identified and documented. At a minimum this should indicate how the physical and logical devices and connections should be handled and identified. Information will be used to update the appropriate URE processes to handle this type of "significant change";
5. review URE processes to determine if documentation exists on how to classify Cyber Assets to be introduced to the CIP environment. Classification process should at a minimum indicate how to identify the different Cyber Asset types (i.e. CCA, EACMS, PACS, PCA) and the URE processes that should be executed to make the Cyber Assets compliant with the CIP Reliability Standards;
6. revise processes as deemed necessary;
7. conduct training for all URE personnel, corporate-wide that work with the CIP environment on the revised and new processes and controls;
8. review all ESPs for Cyber Assets not identified within the ESP in a similar condition as the GPS Cyber Assets. Where additional Cyber Assets are identified, complete the necessary documentation as required by CIP-002 through CIP-009, as an additional milestone;
9. determine internal preventative and detective controls for recognition of "significant change" and potential process execution failures. This would be based on the recommended modifications to the URE processes and the process steps to be included for areas of potential errors. Review and determination of internal controls should be completed after process steps are known and their risk for error in execution can be evaluated; and
10. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R2.1, R2.2, R2.4 (RFC2014014054, RFC2014014055, RFC2014014056)

ReliabilityFirst determined that URE failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs. URE used an overly broad IP address access range space in a firewall rule set such that explicit deny by default was not implemented (R2.1). URE enabled ports on the firewalls that were not

justified as required for operations and for monitoring Cyber Assets within the ESP (R2.2). URE did not demonstrate the use of strong procedural or technical controls at the access points (R2.4).

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failure to limit routable communication across the access points to the ESP weakens a layer of defense required for protection of CCAs. However, the broad IP address range communications were restricted to protected networks that were isolated from external CIP environment networks using firewall technology that only allowed necessary in-bound communications. In addition, the unnecessary enabled ports on the firewalls were isolated to the internal protected networks that did not have external communications to networks outside of the protected networks. Finally, although there was a lack of detailed written documentation on the procedural and technical controls in place for remote access to the control center and substation networks, multiple other safeguards were used including user name and passwords as well as firewall protections.

URE's Mitigation Plan (RFCMIT011115-1) to address these violations and violation IDs RFC2014013312, RFC2014013332, RFC2014013367, discussed in more detail below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. disable identified unnecessary enable ports for occurrences mentioned and update required documentation;
2. review all electronic access points in the URE environment to verify only ports and services required for operation are enabled and are documented;
3. develop documented process that enables validation of information on the change orders (exceptions);
4. complete review of change management for communications with all relevant CIP environment groups;
5. review the potential modifications to the URE change management processes for additional refinements with URE personnel who would start the change management process, review and approve the change request, and then execute the changes to the CIP environment;

6. complete update of change management and change order processes;

7. complete training of all URE personnel involved in the change management and change order processes;

8. complete review of modified change management and change order processes, and identification of areas for improvement including process updates;

9. complete process for collection of IP address/port matrix for use in elimination of broad IP address/port access controls for control center and substation network communications;

10. complete modification of control center and substation network communications;

11. complete creation of detailed procedural and technical controls documentation for control center and substation network communications;

12. complete investigation and approval for multi-factor authentication for remote access;

13. complete implementation of multi-factor authentication for remote access;

14. complete creation of detailed procedural and technical controls documentation for multi-factor authentication; and

15. complete training of applicable URE personnel on multi-factor authentication for remote access.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R2.2 (RFC2014013312, RFC2014013332, RFC2014013367)

ReliabilityFirst determined that URE failed to enable only ports and services required for operations and failed to document accurately the configuration of its ports. This failure was due to ambiguous language in a related change request. In addition, URE's change spreadsheet did not match the actual configuration of several firewalls at URE's control centers. The documented change management procedures in place at the time did not include instructions on communicating changes with the IT department or verifying that the documentation of required configurations were updated.

ReliabilityFirst determined the duration of the violations to be from the date the port documentation was validated as part of the CVA process, through the date URE disabled the unnecessary ports and updated the documentation to reflect accurate configurations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The erroneously enabled port was only for communications between the control houses and there were no communication capabilities in or out of the ESP. Therefore, someone would first have to get through safeguards surrounding the ESP, such as firewalls, before being able to access information through the enabled port. The actual configuration of the firewalls had the correct enabled ports that were required for operations, and the change management documentation had the correct modification information, but the IT department's change spreadsheet was incorrect.

URE's Mitigation Plan (RFCMIT011115-1) to address these violations is described in RFC2014014054, RFC2014014055, and RFC2014014056 above.

CIP-005-1 R4 (RFC2014014169, RFC2014014170, RFC2014014171)

ReliabilityFirst determined that URE failed to verify, during their CVAs, that only ports and services required for operations at access points were enabled. URE discovered a port that allowed access to the ESP at multiple access points that was not required for normal operations. URE should have discovered this port during its previous CVAs.

ReliabilityFirst determined the duration of the violations to be from the date URE was required to comply with CIP-005 R4, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because undocumented ports and services potentially permit unauthorized access to Cyber Assets within an ESP and lack of awareness to review ports and services required for operations at the access points cause exploitable security weaknesses. However, the risk was mitigated because the unnecessary enabled port and service in this instance allowed communications into the ESP to Cyber Assets that were no longer configured to allow connections for the enabled port/service. Therefore, even if an intruder gained access into the ESP through the enabled port, the intruder could not actually obtain information related to CCAs, but could potentially exploit the access point.

URE's Mitigation Plan (RFCMIT011266) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update baseline documentation to include "listening" ports as well as "established" ports/services information;
2. complete review and update of policies and process on required ports/services information;
3. complete review and update of policies and process on what is required for account controls;
4. complete determination of collection method for ports/services information;
5. complete training for all URE personnel on required ports/services and account information and maintenance;
6. complete review and update of the CVA process for establishment of ports/services data, collection of the data, comparison of the data, internal controls to help detect abnormal conditions, and the processes cover all of the CIP requirements;
7. complete execution of the updated CVA process including review of baseline data used for the CVA process to verify the data reflects current operational conditions; and
8. correct the baseline data for instances discovered where the baseline data did not reflect current operational conditions.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R5.1 (RFC2014014051, RFC2014014052, RFC2014014053)

ReliabilityFirst determined that URE failed to ensure its documentation reflected current configurations and processes. The affected assets included GPS data Cyber Assets and ESP access points. The failures were due to a lack of understanding of the CIP requirements for Cyber Asset identification.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE updated its documentation to include the GPS data Cyber Assets in the Cyber Asset lists for both control centers.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The GPS data Cyber Assets are not considered essential to the operation of the control center, resided within an ESP and PSP, are not accessible directly from the internet, but rather only locally accessible, and are therefore protected from unauthorized access. In addition, URE

did document the primary firewall physical and logical ports as ESP access points and housed them within an identified PSP

URE's Mitigation Plan (RFCMIT011265) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update ESP drawing, CCA list and associated documentation (CIP-002 through CIP-009) to include GPS data Cyber Assets and Access Points;
2. complete review of URE processes for "significant change";
3. complete SME interviews and surveys concerning the commissioning processes;
4. issue URE ruling on handling of redundant hardware Cyber Assets;
5. complete review of URE processes used for determination of Cyber Asset classification;
6. revise URE processes used for determination of Cyber Asset classification;
7. complete training of all URE personnel involved in the introduction of Cyber Assets to the CIP environment on the revised URE processes;
8. complete review of all ESPs to identify Cyber Assets that were not previously identified, classified, and/or documented;
9. update URE Cyber Asset lists, diagrams, and associated documentation (CIP-002 through CIP-009) to reflect newly identified Cyber Assets; and
10. develop and implement internal controls to prevent and detect process failures.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R1 (RFC2014014040, RFC2014014041, RFC2014014042)

ReliabilityFirst determined that URE failed to provide the protective measure to a substation radio transmitter system pairs to justify a Technical Feasibility Exception (TFE) under CIP-006 R1.1. The TFE at issue identified a compensating measure requiring the protective measure of encryption on the substation radio transmitter system pairs. However, URE did not enable encryption on the pairs.

ReliabilityFirst determined the duration of the violations to be from the date substation radio transmitter pairs went into production, through the date URE enabled encryption on the devices.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although encryption was not enabled, the fact that remote access was disabled only permitted local access to the devices. The protective measures surrounding the devices, such as an actively monitored PSP and ESP, mitigated the risk of someone gaining unauthorized access to the devices.

URE's Mitigation Plan (RFCMIT011264) to address these violations, and the violations of RFC2014014044, RFC2014014046, RFC2014014047, RFC2014014048, RFC2014014049, RFC2014014050, RFC2014013320, RFC2014013326, and RFC2014013333 described below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. notify URE corporate security executives and management of incident;
2. perform an investigation and interview individuals involved in granting unauthorized physical access;
3. determine and levy disciplinary action against offender;
4. update all PSP URE visitor logbooks with instructions for completing all fields;
5. train offender on CIP access requirements;
6. develop URE visitor and escort training curriculum;
7. notify URE employees, JOCs, and contractors of mandatory URE visitor and escort training;
8. secure cable trays and close all PSP openings more than six inches within operations control rooms;
9. enable encryption on radios;
10. prepare lessons learned from configuration of radios;
11. develop control center physical security inspection;
12. inspect PSP boundaries to ensure CCAs, Non-critical Cyber Assets, and ESPs are within a six-wall boundary;
13. update testing and approval of hardware, firmware and software for CCA devices procedure to ensure TFEs are addressed;
14. develop process for inspecting and correcting URE visitor logbooks entries;

15. place cabinet visitor logbooks in every cabinet PSP; and
16. perform random sample spot-check of newly implemented processes and logbooks;

URE certified that the above Mitigation Plan requirements were completed

CIP-006-3c R1 (RFC2014014044, RFC2014014046, RFC2014014047)

ReliabilityFirst determined that URE failed to have visitor logs for certain cabinets, which are identified PSPs. Technicians were required to contact the control room prior to opening a cabinet, after which the entrance door is unlocked. URE used an electronic lock system to log approved unescorted access, but did not have a separate log within the cabinets themselves.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE put visitor logs into the cabinets.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the cyber locks on the cabinets can be opened only by an individual with an electronic lock system key and unescorted physical access into the PSPs. Therefore, visitors cannot enter the PSP without the assistance of an individual with unescorted access and would be logged as a visitor if they were working on the cabinets.

URE's Mitigation Plan (RFCMIT011264) to address these violations is described in RFC2014014040, RFC2014014041, and RFC2014014042 above.

CIP-006-3c R1 (RFC2014014048, RFC2014014049, RFC2014014050)

ReliabilityFirst determined that URE failed to establish a six-wall border throughout the PSP and failed to document all alternative measures that were in place to secure the PSP. There was an opening in the PSP of URE's operations control room that had a cable tray that ran under a cement floor hallway and connected to a non-PSP room on the other side of the hallway. The non-PSP room had drywall covering the opening on that end, however there was no seal to the cable tray opening on the PSP side.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The operations control room, an identified PSP, has staffing 24 hours a day, seven days a week and the floor panels are difficult to penetrate as they are secured. In addition, the non-PSP location adjacent to the PSP has access controls in place.

URE's Mitigation Plan (RFCMIT011264) to address these violations is described in RFC2014014040, RFC2014014041, and RFC2014014042 above.

CIP-006-3c R1.6 (RFC2014013320, RFC2014013326, RFC2014013333)

ReliabilityFirst determined that URE failed to log all required information relating to visitors and failed to have the designated individual provide continuous escorted access to certain visitors. There were instances where details such as time in, time out, or reason for visit were missing in the URE visitor logbooks. Additionally, a JOC employee allowed subcontractors access into the URE control house and then left the visitors in the control house PSP without an official escort.

ReliabilityFirst determined the duration of the violation to be from the first date the logbook entries were incomplete, through when URE completed its mitigation activities for these violations.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. In the nine instances identified, the visitors' names were in the visitor logbooks and there is no indication that the individuals were not escorted. Although the official JOC escort did not stay with certain visitors, there were unofficial escorts with the individuals, thus reducing any risk that the individuals could use equipment in a way that would put the BPS at risk or allow access to confidential information.

URE's Mitigation Plans (RFCMIT010968 for RFC2014013320, RFCMIT010966 for RFC2014013326, and RFCMIT010967 for RFC2014013333) to address these violations were submitted to ReliabilityFirst. In addition to these Mitigation Plans, certain mitigation activities taken as a part of RFCMIT011264, described in RFC2014014040, RFC2014014041, and RFC2014014042 above, also mitigated these violations.

URE's Mitigation Plan required URE to:

1. develop training for visitor log book usage;
2. notify JOCs of the mandatory training; and
3. conduct training with URE employees and contractors.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R1 (RFC2014013309)

ReliabilityFirst determined that URE failed to have all Cyber Assets within an identified PSP with an enclosed border. Cabling for the ESP between the PSPs at a URE substation was not inside an encased conduit nor was it inside a controlled six-wall protection boundary.

ReliabilityFirst determined the duration of the violation to be from the date URE needed to comply with the Standard, through when URE installed conduit encasing wiring between the PSPs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because the PSPs at issue were close in proximity in a single URE building that was enclosed with a fenced boundary, and thus there were barriers in place to protect the cabling from intruders.

URE's Mitigation Plan (RFCMIT010804) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. install conduit encasing wiring between the two PSPs; and
2. publish its substation inspection process document and distribute to key stakeholders and SMEs.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that URE's Mitigation Plan was complete.

CIP-006-3c R2.2 (RFC2014014037, RFC2014014038, RFC2014014039)

ReliabilityFirst determined that URE failed to provide sufficient evidence that the virtual machine hosts and virtual machine chassis were afforded the protective measures identified in CIP-006-3c R2.2. URE properly identified virtual machines containing PACS applications as PACS with all the appropriate protection controls, however, the virtual machine host running the virtual machine clients were not identified as PACS. The virtual machine host is an integral part of the client and must be afforded the measures as required by the Standard. The failure was due to a lack of training and knowledge on the Standard and requirement.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not implement all of the protective measures on the virtual machine hosts as required by CIP-006-3c R2.2, there were multiple other protective measures in place that reduced the risk of unauthorized access to the virtual machine hosts. For example, the virtual machine hosts were inside a PSP with multiple layers of firewalls protecting the hosts; URE performed patching on the hosts and hardware; URE monitored the hosts for operational and security alarms; and all individuals having access to the virtual machine hosts were vetted in accordance with CIP-004 R3.

URE's Mitigation Plan (RFCMIT011283) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. complete review of corporate policies on virtual machines usage and how it applies to the CIP environment;
2. complete catalog of existing virtual machines usage in the CIP environment;
3. complete creation of migration plan if required to separate CIP and non-CIP virtual machines clients;
4. complete development of standard for virtual machines usage in the CIP environment;
5. complete review of change management process for modifications related to virtual machines usage;
6. complete interviews with SMEs, Standard owners, and IT infrastructure on process and standard modifications for virtual machines technology;
7. complete creation and/or update of URE CIP program policies, standards, and processes to ensure compliance of virtual machines technology;
8. train personnel on updated policies, standards, and processes;
9. modify designs to virtual machines technology usage if required to separate virtual machines clients.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R5 (RFC2015014591)

ReliabilityFirst determined that URE failed to review immediately and handle unauthorized access attempts in accordance with the procedures specified in CIP-008-3. An employee of a URE JOC arrived at a URE substation and attempted access to the switchyard by using the JOC-issued access badge. The badge created an alarm that was reported to the URE security command center. The employee then used an issued electronic key system to gain access to the control house twice, although the key was not programed for the substation and therefore set off an alarm. The control house door lock was defective and allowed enough movement when turned in concert with the electronic key system to allow the door to be opened. Once inside the control house, the employee failed to complete all the required fields of the logbook. The employee remained in the control house for eight minutes, exiting and remaining within the switchyard for approximately 30 minutes. URE security officers acknowledged the alarms, determined they were caused by a JOC employee, and failed to investigate the matter further.

ReliabilityFirst determined the duration of the violation to be from the date the URE failed to respond immediately to the alarm conditions, through when URE completed investigation of the alarm conditions.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Even though there were security alarms, URE security personnel did not timely investigate the alarms and conduct due diligence as required by CIP-006-3c R5. Permitting someone without authorized access to access a PSP puts the BPS at risk of that individual tampering with equipment or compromising CCA information in a way that could harm the reliability of the BPS. The security officer immediately recognized the alarms, and thus was aware that the individual was accessing the PSP. In addition, the employee was an active employee, in good standing, with unescorted physical access into URE non-CIP substations, thereby reducing the likelihood that he would have used the access in a way to put the BPS at risk. Finally, during the investigation of the alarms, URE's IT department performed an inspection of the network and identified no abnormalities.

URE's Mitigation Plan (RFCMIT011409) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. interview, reprimand, and counsel the URE on-duty security officer;
2. conduct an internal thorough investigation of the response to the alarm;

3. disseminate an awareness and training communication and follow-up correspondence reiterating the alarm process and addressing additional inquiries and points of clarification to all personnel at the security command center concerning the incident;
4. replace the locking mechanism on the door latch;
5. complete the review and update (if necessary) its physical access process to ensure the accuracy of its directives for alarm investigations and responses;
6. begin an extent of conditions system-wide inspection, assessment, and test to determine if there were any additional defective locking mechanisms at other URE substations; and
7. complete the training on its physical access process for all its security personnel responsible for the monitoring of URE's physical security system.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R1.3 (RFC2014013322, RFC2014013327, RFC2014013334)

ReliabilityFirst determined that URE failed to document test results for changes or new Cyber Assets. URE did not complete a control and configuration management work form for certain physical security Cyber Assets after reclassifying an URE substation from a non-CIP site to a CIP site, and therefore failed to document test results for the new Cyber Assets introduced into a CIP environment. In addition, URE replaced some existing terminal servers that required the use of terminal servers. The personnel installing these assets did not correctly view the replacement as a significant change to the CIP environment. Finally, URE installed new servers-based Cyber Assets that utilized non-approved versions of one application. URE assigned the task for updating the system version but the assigned team never completed the upgrade, and therefore URE personnel did not verify the version in URE's patch version control document.

ReliabilityFirst determined the duration of the violations to be from the date the first Cyber Assets were commissioned, through when URE updated the application to the correct version, conducted testing, and provided documentation as required by URE processes.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, the risk was increased because the newly commissioned Cyber Assets may have caused system instabilities when the new Cyber Assets are placed into production without adequate testing. This may have caused unforeseen vulnerabilities, such as unnecessary open ports or lack of patches or ineffective antivirus software.

URE's Mitigation Plan (RFCMIT011280) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. complete the Cyber Asset commissioning process for the terminal servers;
2. update the application to the correct version, conduct testing and provide documentation as required by URE processes;
3. create and distribute a survey for suggestions on improving process flow and execution;
4. interview SMEs involved in Cyber Asset commissioning to provide feedback and enhancements for the process(es) being developed;
5. review URE processes for the definition of "change" and "significant change" and revise to cover potential conditions, including "like-for-like" replacements, related to the CIP environment;
6. assess URE processes and procedures to include procurement, risk assessment, asset management, and supply chain trigger points and hand-offs to the testing process;
7. create guidelines for defining and documenting the non-production test environment used for CIP-007 R1 significant change testing;
8. revise URE processes and procedures to remove any potential confusion on execution and capture the recommendations from the SME interviews and survey that add-value and provide efficiency;
9. create internal preventative and detective controls for recognition of "significant changes" and actual process execution failures; and
10. conduct training for all URE personnel that work in or affect the CIP environment on the resulting revised and new processes and controls.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3 R2, R2.1, R2.2 (RFC2014013335, RFC2014014072, RFC2014014073, RFC2014014074, RFC2013012767, RFC2014013310, RFC2014013313, RFC2014013315)

ReliabilityFirst determined that URE failed to ensure that only ports and services required for normal or emergency operations were enabled and/or that other ports and services were disabled on Cyber Assets within the ESP prior to production.

During URE's CVA, it discovered an undocumented port and service enabled on a relay and that its ports and services documentation for the Windows systems in the entire CIP environment did not address the required services running on the Cyber Assets without listening ports. URE also discovered an open port and associated service on an Ethernet switch at a transmission substation.

ReliabilityFirst determined the duration of these violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

URE installed modules into the CIP environment with default IP ports enabled. At the time, URE did not have a documented baseline of required ports and services. The enabled IP ports were identified during the CVA, however it did not specify that the review of the enabled ports and services against documentation of required ports and services was applicable to the Cyber Assets.

ReliabilityFirst determined the duration of these violations to be from the date URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

URE discovered an enabled port between a remote terminal unit (RTU) and the annunciator at a URE substation that was not required for operation of the two devices. In addition, during the CVA, URE discovered that a port was enabled on several wireless radios that connect transformer monitoring systems from the substation yard back to the control building. This port was not required for operation of the radios.

ReliabilityFirst determined the duration of these violations to be from when URE enabled the unnecessary ports on the radios, through when URE completed its Mitigation Plan.

URE conducted CIP baseline testing and implementation of an interface card. URE determined the card came configured from the factory with IP ports enabled that are not necessary and should have been disabled prior to installation.

ReliabilityFirst determined the duration of this violation to be from when URE commissioned and placed into service the interface card with unnecessary enabled ports, through when URE disabled the ports.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE's not ensuring that it enabled only ports and services required for normal or emergency operations across relays, systems, annunciators, PACS, switches and interface card devices indicated a programmatic failure. In addition, these issues cumulatively create vulnerabilities that

expose the systems to a higher risk of compromise by potentially allowing more channels for undetected access into URE's critical systems. Finally, insufficient documentation of the required ports and services on essential Cyber Assets can result in not ensuring only required ports and services are enabled. Given these risks from multiple issues and the duration, the violations posed a serious and substantial risk to the reliability of the BPS.

Due to the timing of the Self-Reports, URE's Mitigation Plan (RFCMIT010171) to address the violation of RFC2013012767 was submitted to ReliabilityFirst prior to the Mitigation Plan addressing the remaining violations in this section.

URE's Mitigation Plan required URE to create an IP Ports and Services procedure for the specific Cyber Asset type and disable the unnecessary ports on the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

ReliabilityFirst verified that the URE Mitigation Plan was complete.

URE's Mitigation Plan (RFCMIT011278) to address the violations of RFC2014013335, RFC2014014072, RFC2014014073, RFC2014014074, RFC2014013310, RFC2014013313, and RFC2014013315 was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. correct the identified unnecessary enabled ports and services which should have been disabled and update appropriate documentation;
2. review TFEs currently in place to ensure they accurately represent URE's Cyber Asset capabilities;
3. submit or revise TFEs currently in place to address any misrepresentation of URE's Cyber Asset capabilities;
4. conduct SME interviews for all functional groups involved with Cyber Asset commissioning and vulnerability assessments to improve process flow and execution;
5. conduct a thorough review of all URE Cyber Assets within the CIP environment to verify that only the ports and services required for normal operation are enabled and the documentation of the required ports and services is correct for all devices in the CIP environment. URE would then correct the identified unnecessary enabled ports and update of the appropriate documentation;

6. review and update the processes for Cyber Asset commissioning and vulnerability assessments based on feedback from the interviews with the SMEs from all functional groups and train all URE personnel involved in the Cyber Asset commissioning and vulnerability assessments on the process changes; and
7. review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R3.1, R3.2 (RFC2014013321, RFC2014013328, RFC2014013336, RFC2014014078, RFC2014014079, RFC2014014080)

ReliabilityFirst determined that URE failed to perform an assessment of security patches and security upgrades within 30 days of availability for all Cyber Assets within the ESP and failed to document the implementation of security patches for all Cyber Assets within the ESP.

URE did not evaluate security patches for the transmission management system's (TMS) servers within the 30-day timeframe. In addition, during a mock audit, URE discovered additional security patches for multiple Cyber Assets were not evaluated within the 30-day required timeframe.

URE also discovered that the PACS Cyber Assets installed with the cyber audit web application did not have patching capabilities as required by CIP-007-3a R3 and URE failed to file a TFE for those assets and failed to document compensating measures. URE had also placed terminal servers into production without the ability to implement patches and that did not have the capability for patching without being set back to the original equipment manufacturer. URE should have created and filed a TFE and compensation controls for these servers.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because failing to timely assess and implement security patches, especially on critical systems, can lead to increased vulnerability to a cyber-attack that could compromise the BPS. However, URE had compensating controls in place while the Cyber Assets were not patched, or where systems could not be patched. These compensating controls included regular monitoring of the systems, with the logs reviewed on a daily basis, and automated alerts for predefined conditions such as excessive login failures of two or more within a short period.

URE's Mitigation Plan (RFCMIT011263) to address this violation was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. file necessary TFEs for SPT and PACS affected systems;
2. document all applicable operating system and application vendors and their associated patch release schedules and sources;
3. upgrade relevant corporate security PACS servers with the web application to an operating system and application version that supports security patching;
4. develop internal controls to assist in verification of proper process execution with emphasis on preventative controls to catch processing errors at the time of execution;
5. review and update URE policies, processes, and procedures regarding patching to ensure compliance with CIP-007-3 R3. The updated policies, processes, and procedures will:
    a. indicate that original equipment manufacturer sources that should be used for notification of patch releases;
    b. indicate that a 30-day timeframe is required for patch evaluation after original equipment manufacturer release;
    c. address third-party supplier situations;
    d. require inclusion in evaluation documentation the purpose of the patch (i.e. security fix or new features), the applicability, and any effect identified as a result of patching; and
    e. require recommendations within 30 days of the patch evaluation to the asset owner(s).
6. implement a process to indicate source of security patches enforcing that the start of the 30-day timer will be the original equipment manufacturer security patch release date for Cyber Assets within the CIP environment;
7. create a patch evaluation, testing, and deployment schedule to reduce the patch cycle from six months to 90 days;
8. place applicable systems under URE patching process for correct evaluations and installation;
9. provide training to ensure that URE personnel responsible for patch evaluation are aware of original equipment manufacturer patch sources and receive notification of new patch releases and provide training to all URE personnel involved in patching for the CIP environment on all created and revised policies and processes; and

10. verify correct execution of patching.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R4, R4.1 (RFC2014013692, RFC2014013694, RFC2014013696)

ReliabilityFirst determined that URE failed to document compensating measures. While preparing for its Compliance Audit, URE discovered its PACS Cyber Assets that were installed with the web application did not support malware protection software as required by CIP-007 R4. URE had not filed for a TFE or documented compensating measures for these PACS Cyber Assets. In addition, URE discovered SPT terminal servers it had placed into production without applying malware prevention software.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not document compensating measures, mitigating measures were implemented during commissioning of the PACS Cyber Assets. Physical and cyber access to the PACS Cyber Assets is limited, along with full logging enabled, for significant events such as login attempts and failures. Ports and services are controlled by the corporate firewall access control lists. The PACS Cyber Assets reside on a secure and separate virtual local area network. The SPT terminal servers did not have external communication capabilities since they were configured to only communicate within the ESP, thereby reducing the possibility of a compromise.

URE's Mitigation Plan (RFCMIT011262) to address these violations, as well as for the violations RFC2014014069, RFC2014014070, and RFC2014014071 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. review the need for and file necessary malware TFEs for SPTs and PACS;
2. upgrade systems to an operating system and application version that will support malware prevention software;
3. conduct SME interviews to gain insight and solicit recommendations to improve malware signature processing;

4. review all URE policies, processes, and procedures regarding malware protection and revise to indicate clearly malware protection is required for the CIP environment along with requisites of installation and testing of applied signatures, or that a TFE and mitigating protections are required;
5. establish and implement internal controls to verify malware protection is applied to all Cyber Assets that have the capabilities, malware signatures are applied within the prescribed timeframe, and compensating controls are in place;
6. provide training on new or revised processes to all URE personnel involved with malware protection; and
7. conduct review process execution.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R4, R4.2 (RFC2014014069, RFC2014014070, RFC2014014071)

ReliabilityFirst determined that URE failed to document compensating measures for PACS Cyber Assets, and failed to document or implement a process to update antivirus and malware prevention "signatures". URE was unable to provide evidence regarding the testing of malware prevention software signatures as required by CIP-007 R4.2.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because although URE could not provide malware signature update documentation, they have the processes and procedures in place for the testing and installation of signature files on Cyber Assets, and indicated that signatures were updated per the current process.

URE's Mitigation Plan (RFCMIT011262) is discussed with violations RFC2014013692, RFC2014013694, and RFC2014013696 above.

CIP-007-3 R5.1.2, R5.2.1, R5.2.2, and R5.2.3 (RFC2014014066, RFC2014014067, RFC2014014068)

ReliabilityFirst determined that URE failed to produce logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days. In addition, URE failed to

have documentation for a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges.

Specifically, URE could not demonstrate sufficient detail on account activity for a sample size of Cyber Assets or provide implementation of a policy and management of shared and default accounts for PACS or the account used by the TMS department. URE did not have information for shared administrator accounts related to electronic lock PACS, could not provide documentation for a policy that includes the removal, disabling, or renaming of shared accounts, and did not provide documentation identifying individuals with access to shared accounts. Finally, URE could not provide documentation that explicitly identifies a policy for managing the use of shared accounts that limits access to only those with authorization, or an audit trail of the account usage and maintenance.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, the violations span across multiple systems and accounts in URE's network and inadequate audit trails of user actions on CCAs can lead to missing cyber security events and inadequate shared account management can lead to inadvertent use of URE's CCAs, which can result in compromise of CCAs.

URE's Mitigation Plan (RFCMIT011281) to address these violations, and violations RFC2014013428, RFC2014014009, RFC2014013323, RFC2014013329, and RFC2014014008 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. file appropriate TFEs for the SPT terminal servers;
2. correct default password configurations on the affected devices;
3. update the account information of URE personnel with knowledge of the accounts;
4. review all processes used the by URE departments for account management to determine how the processes satisfy CIP-007-3a R5 and identify in the processes;
5. review all tools used by URE departments for account management to determine how the tools satisfy CIP-007-3a R5, CIP-003-3 R4, and CIP-003-3 R5 and determine if there are gaps in the toolsets;

6. conduct SME interviews for input on current process execution, problems with the execution, and suggestions on process improvements;
7. create standardized processes across departments;
8. identify standardized tools to handle the account management processes;
9. develop internal controls to identify process execution exceptions, escalation of the exceptions for proper handling, identification of new process requirements, and continuous improvement of the process, and methods to enable adherence to process requirements and consequences for failure to follow the processes;
10. identify and review the usage and documentation of default, root, administrator, and shared accounts in the URE departments for account management and determine how the use of these accounts can be suspended by implementing other accounts, or document special account usage and controls per CIP-007-3a R5.1 and R5.2;
11. review methods used by the URE departments for account management for documenting and recording account usage per CIP-007-3a R5.1.3 and R5.2.3. Where activity usage account is not documented or recorded in sufficient detail, URE would develop methods to collect the information. In instances where the account cannot be disabled, URE would create the necessary documentation capturing the vendor limitations and compensating controls to maintain awareness of account usage;
12. conduct training for URE personnel in the URE departments for account management on the standardized processes and tools; and
13. review process execution item.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R5 (RFC2014013428, RFC2014014009, RFC2014013323, RFC2014013329, RFC2014014008)

ReliabilityFirst determined that URE failed to implement and document technical and procedural controls that enforce access authorization of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

While preparing for its CIP Compliance Audit, URE discovered several incomplete workforms. URE personnel did not correctly document information on the workforms because URE process documentation was unclear (First Instance). In addition, URE discovered that it did not have sufficient evidence to validate system level access privileges of user accounts on an annual basis. The evidence

did not demonstrate that the URE accounts being reviewed were actually checked against the systems on which the accounts were provisioned to ensure the accounts existed and were provisioned correctly (Second Instance). URE also discovered that during its system transition from a corporate security portal to URE's access management system, some of the roles and perimeters were lost from personnel profiles. As a result, when an individual was terminated, there access privileges were not documented as revoked although actual access was revoked (Third Instance).

During its CVA, URE discovered that for two of three shared accounts, passwords and usernames on four Ethernet switches that were inadvertently reset to the factory default usernames and passwords. The passwords were not strong or meet the requirements of CIP-007 R5 (Fourth Instance). In addition, URE discovered that default passwords were on several relays at URE substations—in each device, one shared account was configured with the factory default password and these default passwords were not strong and did not meet URE's Cyber Asset password policy (Fifth Instance).

Finally, URE discovered that SPT terminal servers were placed into production without the application of URE processes for account management. URE also did not request a TFE for these assets. URE personnel did not view the replacement of the assets as a "significant change" to the CIP environment and therefore did not assess, classify, or commission the SPT terminal servers as CCAs (Sixth Instance).

ReliabilityFirst determined the duration of the violations to be from the date the oldest asset at issue was commissioned, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because the failure to implement and document technical and procedural controls that enforce access authentication of all user activity increases the risk of unauthorized access and thus potential compromise of CCAs.

The risk was mitigated for the following reasons. Regarding the First Instance, URE properly configured and recorded the actual account, but URE did not have a complete workform as required by their processes. Regarding the Second Instance, the accounts were in fact provisioned correctly and URE's defense-in-depth strategies reduced the risk of someone accessing the systems for improper purposes. Regarding the Third Instance, logical access was removed from the Cyber Assets. Regarding the Fourth Instance, the Ethernet switches did not have external connectivity or remote management connectivity to allow for potential compromise. Regarding the Fifth Instance, the default passwords were in the upper access tier of the relays, thus someone would have to first use a password for the lower tier to gain access, and the lower tier password was strong. In addition, access to the relays required physical

access, which was protected by a PSP. Finally, regarding the Sixth Instance, the SPT Terminal Servers reside within a PSP and an ESP, thus restricting access to only authorized personnel.

URE's Mitigation Plan (RFCMIT011281) is discussed with violations RFC2014014066, RFC2014014067, and RFC2014014068 above.

CIP-007-3a R6.1, R6.4 (RFC2014014063, RFC2014014064, RFC2014014065)

ReliabilityFirst determined that URE failed to produce evidence that logs of system events relating to cyber security were maintained and reviewed for a minimum of 90 days. The violation affected devices owned by the corporate security, IT services, and transmission systems management functional groups. These groups could not provide evidence regarding what logs were reviewed, how they were reviewed, or when the reviews were completed. The failure was due to the fact there were multiple logging mechanisms across the organization that led to inconsistent processes.

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, for the sample that ReliabilityFirst reviewed, URE could not provide evidence for almost half of the devices regarding which logs they were reviewing, how they were reviewing the logs, or when they completed the reviews. System event logs related to Cyber Assets are important to detect and prevent any security incidents. Lack of an adequate logging mechanism and periodic review of relevant logs significantly weakens URE's position to detect, investigate, and resolve security events

URE's Mitigation Plan (RFCMIT011261) to address these violations, and the violations of RFC2014013324, RFC2014013330, RFC2014013338 discussed below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. file necessary TFEs for affected SPT systems that require a TFE;
2. review logging capabilities for the current logging tools and CIP environment to determine a master tool or set of tools that can be used to collect Cyber Asset logs with the goals of reducing the number of logging tools to a minimum. URE will ensure that the master logging and analysis system has capabilities for automated log analysis and alert triggers that are customizable to meet URE and CIP security requirements;

3. determine the requirements to establish the URE cyber security operation center as the single source for log collection and analysis;
4. review current URE processes used for log collection and analysis to determine which meet the CIP security Standard requirements and can be used in the creation of a methodology and processes to be used by the URE cyber security operation center or the four departments if the URE cyber security operation center cannot be setup as the central logging and analysis center;
5. conduct interviews with logging and log analysis SMEs to determine possible improvements in process execution for the different processes to assist in arriving at a single set of corporate-wide processes;
6. determine log review and automated alerting criteria to cover the requirements for CIP Version 3 and Version 5;
7. generate recommendation on corporate-wide master logging and analysis tool set for review and approval using the results of the logging tool review, process review, SME interviews, and logging and analysis criteria;
8. generate process documentation based on the process reviews, SME interviews, development of manual and automated analysis criteria, and handling of potential security events;
9. implement the methodology of logging and standardized tool set;
10. train all URE personnel on the appropriate logging methods and tools used by each group and cyber security operation center staff to handle collected log data; and
11. review log collection an analysis after deployment to verify correct execution and additional areas of improvement.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R6.5 (RFC2014013324, RFC2014013330, RFC2014013338)

ReliabilityFirst determined that URE failed to implement and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. The violation included incomplete workforms for log reviews and SPT terminal servers placed into service without the capability of generating logs.

ReliabilityFirst determined the duration of the violations to be from the date URE needed to comply with the Standard, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The security event logs for the Cyber Assets in question were reviewed in a timely and consistent manner—only the workform was not completed. The SPT terminal servers do not have external communication capabilities since they were configured to only communicate within the ESP, thereby reducing the possibility of a compromise.

URE's Mitigation Plan (RFCMIT011261) is discussed in violations RFC2014014063, RFC2014014064, and RFC2014014065 above.

CIP-007-3 R8.2, R8.3 (RFC2014014060, RFC2014014061, RFC2014014062)

ReliabilityFirst determined that URE failed to execute its CVA to verify that only ports and services required for operation were enabled nor did it review controls for default accounts for Energy Management Systems (EMS) and PACS. While URE was able to demonstrate some reviews of ports and service and default accounts, it was not able to do so for all Cyber Assets. URE lacked effective asset and configuration management and verification controls, had incomplete processes, and inadequately trained personnel.

ReliabilityFirst determined the duration of the violations to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, not reviewing enabled ports and services can create unidentified vulnerabilities into the network by creating possible access points into the network, which increases risk of unauthorized access to critical systems. In addition, a review of default accounts to verify they have been disabled or renamed and the password changed is critical to protecting Cyber Assets. Finally, not reviewing default accounts potentially allows external personnel with knowledge of default credentials to gain access to critical systems.

URE's Mitigation Plan (RFCMIT011260) to address these violations, and the violations RFC2014013325, RFC2014013331, and RFC2014013339 below, was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. update baseline documentation to include "listening" ports as well as "established" ports and services information;

2. review and update URE policies and processes on what is required for documentation of ports and services information for all Cyber Assets and require all URE departments to use the same policies and procedures for recording ports and services information;
3. review and update policies and process on what is required for default, root, administrative, and other special account controls and require all URE departments to use the same policies and procedures for recording account information;
4. determine method for collection and documentation of all ports and services required for normal operation (i.e. baseline);
5. execute training for all URE personnel responsible for CIP environment ports and services and default, root, administrative, and other special accounts on the required information and maintenance of the information;
6. review and update the URE CVA process for gaps in information required and require all URE departments to use the same process for review of default, root, administrative, and other special accounts. URE would develop internal controls to trap for collection errors and comparison errors and streamline the collection of the required data and will consider and emphasize automated methods;
7. execute the updated CVA process, which will include a review all CVA baseline data and verification that data reflects the current operational conditions; and
8. correct the baseline data for instances discovered during the CVA activities where the baseline data did not reflect current operational conditions.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R8.3, R8.4 (RFC2014013325, RFC2014013331, RFC2014013339)

ReliabilityFirst determined that URE failed to include evidence of a review of controls for default accounts in its CVA documentation. The violation related to Cyber Assets owned by URE departments for engineering and asset management, corporate security, and IT services.

ReliabilityFirst determined the duration of the violations to be from the date of URE's CVA, through when URE completed its Mitigation Plan.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. Specifically, a review of default accounts to verify they have been disabled or renamed and

the password changed is critical to protecting Cyber Assets. Not reviewing default accounts potentially allows external personnel with knowledge of default credentials to potentially gain access of critical systems.

URE's Mitigation Plan (RFCMIT011260) is described in RFC2014014060, RFC2014014061, and RFC2014014062 above.

CIP-008-3 R1.6 (RFC2014014075, RFC2014014076, RFC2014014077)

ReliabilityFirst determined that URE failed to complete several sections of its Cyber Security Incident Response Plan checklist or incorporate lessons learned from an actual cyber security incident into its Response Plan

ReliabilityFirst determined the duration of the violations to be from the last day of the previous URE CIP Compliance Audit, through when URE updated its Response Plan.

ReliabilityFirst determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was increased because the Cyber Security Incident Response Plan needs to be completely tested to adjust the Response Plan as necessary based on the test so that it can ensure its Response Plan will be effective in case of a security incident. However, the Response Plan otherwise met the CIP-008-3 requirements, and URE at least attempted to perform an annual test of the Response Plan, thus reducing the risk that the plan will be ineffective in case of an actual security incident.

URE's Mitigation Plan (RFCMIT011259) to address these violations was submitted to ReliabilityFirst.

URE's Mitigation Plan required URE to:

1. conduct a table-top exercise observers in attendance with a goal of acquiring a different perspective and input for the lessons learned;
2. hold a follow-up meeting to review and discuss lessons learned with all participants and observers;
3. prepare a lessons learned final report describing the ideas and outcome of the exercise, and the discussions during the lessons learned meeting;
4. update the Response Plan to incorporate the exercise results and lessons learned from the final report;

5. add clarifying instructions to the response checklist that are consistent;
6. supplement the Response Plan with a matrix for systems and required responses;
7. establish role-specific evidentiary records by creating a tracking system for recording actions performed by each URE group during execution of the Response Plan;
8. develop a role specific training course for the cyber security incident response team participants; and
9. conduct a role-specific training course for the cyber security incident response team participants.

URE certified that the above Mitigation Plan requirements were completed.

CIP-009-3 R5 (RFC2014013378, RFC2014013379)

ReliabilityFirst determined that URE failed to test information on backup media that is essential to recovery annually. The violation involved multiple Cyber Asset classes at multiple locations—the information was not available in the location specified as required by the Recovery Plan.

ReliabilityFirst determined the duration of the violations to be from when URE updated its Recovery Plan but failed to validate that the recovery information was available at the location identified for certain CCAs, through when URE validated the missing information.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the BPS. Specifically, in order to accomplish the restoration of functionality of a CCA, URE need to obtain the essential information to recover the asset and reestablish the functionality previously served by the failed asset. If URE would lose a CCA at one of these locations, they could rebuild it from scratch, but if the information to recover the asset is not identified and available, it will hinder timely recovery of that Cyber Asset. Depending on the CCA and the function it performs, this may cause serious harm to a critical location, and in turn the BPS.

The risk was partially mitigated because URE could restore the CCA functionality by replacing the failed Cyber Assets. As an example, a relay, for which the function is protecting a transmission line, has an alarm indicative of a malfunction. The URE would investigate that alarm with onsite recovery practices described as part of their recovery plans. In addition, to ensure reliability of the BPS, URE follow operational procedures to replace the Cyber Asset with an equivalent device. They execute this by following the change and configuration management practices required by the CIP Standards.

The URE Mitigation Plan (RFCMIT010801 and RFCMIT010801) to address these violations were submitted to ReliabilityFirst.

The URE Mitigation Plan required URE to:

1. conduct a root cause analysis;
2. validate availability for the missing Cyber Asset recovery information; and
3. conduct a comprehensive review of recovery information for all Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of four hundred twenty-five thousand dollars (425,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors, additional detail on each of the below factors is included in the Settlement Agreement:

1. URE has a compliance history that includes instances of noncompliance with NERC Reliability Standards. ReliabilityFirst considered these prior violations as aggravating factors in the penalty determination;
2. URE has completed all mitigating actions for all violations, and as a result, ReliabilityFirst has determined that URE is appropriately managing, monitoring, and mitigating the risk posed by the violations;
3. although URE's issues that are more significant were mostly centralized in specific areas, URE went above and beyond the actions required to mitigate the violations and committed to overhaul the entire CIP Compliance Program in order to better coordinate and streamline processes and enhance overall security posture. ReliabilityFirst awarded mitigating credit for these measures;
4. ReliabilityFirst will perform a Spot Check of URE. This Spot Check will include two components. First, the Spot Check will include an evaluation of evidence related to implementation of the above and beyond action items. Second, the Spot Check will include a review of URE's current state of compliance for a targeted sample of the CIP Reliability Standard Requirements;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. of the 70 discrete sets of facts and circumstances included in the violations, ReliabilityFirst determined that 24 posed a minimal risk, 28 posed a moderate risk, and the 18 remaining posed a serious and substantial risk to the reliability of the BPS;
8. URE completed several of the remediation activities described above before ReliabilityFirst conducted the Compliance Audit. ReliabilityFirst considered URE's response to the violations to be exemplary, so it awarded a significant amount of credit to encourage similar responses by URE and other registered entities in the future; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the monetary penalty of four hundred twenty-five thousand dollars ($425,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 11, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

In reaching this determination, the NERC BOTCC considered the factors considered by ReliabilityFirst as listed above, as well as the following factors:

1. ReliabilityFirst worked collaboratively with URE to implement mitigation and above-and-beyond solutions that should help URE maintain secure and reliable operations for at least the next few years;
2. while ReliabilityFirst favored expenditures on such solutions over a higher monetary penalty, the $425,000 penalty is significant;
3. beyond the monetary penalty, the Spot Check will allow ReliabilityFirst to assure that URE is maintaining the improved systems and processes implanted during the mitigation process;
4. the Settlement Agreement balances the goals of deterring undesired conduct by registered entities and encouraging aggressive mitigation, above-and-beyond activities, and cooperation by registered entities; and
5. URE's conduct in completing all mitigating actions within nine months, maintaining constant communication and transparency with regional staff, contrasts with the conduct of entities receiving a larger assessed penalty with a similar number of violations.[8]

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of four hundred twenty-five thousand dollars ($425,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[8] *See, e.g.*, NP14-48-000 covering 100 violations of CIP Standards for a total penalty of $625,000.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Deputy General Counsel, Vice President of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0682 216-503-9207 facsimile bob.wargo@rfirst.org

	Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0683 216-503-9207 facsimile jason.blake@rfirst.org Kristen M. Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-06769 216-503-9207 facsimile kristen.senk@rfirst.org

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Deputy General Counsel, Vice President of
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

October 29, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of NERC Reliability Standards. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred sixty thousand dollars ($160,000), in addition to other

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC2013012102	CIP-002-1	R3	High/ High	CA	$160,000
WECC2013012387	CIP-003-1	R6	Lower/ Severe	SC	
WECC2012010893	CIP-004-1	R3	Medium/ Severe	SR	
WECC2013012363	CIP-004-2	R4	Lower/ High	SR	
WECC2013012357	CIP-005-1	R1	Medium/ Severe	SR	
WECC2013012459	CIP-005-3	R4	Medium/ Severe	CA	
WECC2013012465	CIP-006-3c	R1, R1.1	Medium/ Severe	CA	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC2013012466	CIP-006-3a	R2, R2.2	Medium/ Severe	CA	$160,000
WECC2014013599	CIP-007-1	R8	Medium/ Severe	SC	
WECC2013012460	CIP-007-3a	R8	Medium/ Severe	CA	

WECC2013012102 CIP-002-1 R3 - OVERVIEW

WECC determined that URE failed to update its list of all Critical Cyber Assets (CCAs) as necessary. Specifically, URE's list of all CCAs contained a number of inaccuracies because URE failed to update the list annually, as required. Further, URE failed to update its master CCA list within 30 days after it decommissioned certain servers.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). All mislabeled and otherwise misidentified devices resided within the Electronic Security Perimeter (ESP) and Physical Security Perimeters (PSPs) and received the logical and physical protections applicable to CCAs. URE appropriately removed the two server devices from service. Physical and logical access to the CCAs is limited to authorized URE personnel who completed personnel risk assessments (PRAs) and cyber security training. URE logs and monitors physical and logical access to the CCAs. Finally, URE personnel are notified of unauthorized access attempts.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE removed the servers from the master CCA list.

URE submitted its Mitigation Plan designated WECCMIT011213 to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the servers from the master CCA list;
2. restructure its change management as it relates to the CCA list;
3. assign additional personnel to assist the CCA list process owner;
4. enhance existing change management procedure to ensure the CCA list is updated prior to testing the change and train resources on the revised procedures and controls;

5. enhance existing information technology NERC CIP implementation checklist to ensure CCA changes are captured; and
6. develop an operational guideline for conducting annual physical asset inventory verification.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012387 CIP-003-1 R6 - OVERVIEW

WECC determined that URE failed to create change control tickets for patches deployed on Cyber Assets. Approximately half of the devices are classified as CCAs and the remaining devices are electronic access control and monitoring (EACM) devices and Physical Access Control System (PACS) devices, i.e. non-critical Cyber Assets. The devices in scope include printers, workstations, servers, redundant process controllers, scanners, switches, and routers.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because failure to follow change control and configuration management processes for the upgrades could have exposed the CCA hardware and software components to cyber vulnerabilities.

The risk was mitigated because URE does have an established and documented process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software. In addition, URE completed testing on the patches before implementing the patches and gathered and approved testing evidence before it made changes to the devices. Finally, URE's networks are secured, private networks configured specifically to restrict access by default, which do not have access to either URE's intranet or the Internet.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010203 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a security management controls document identifying the requirements when change management/ configuration management is needed. The document includes an attachment toolkit containing all the instructions and forms required to complete and finalize a change record;

2. develop several documents to address the deficiencies, including security management control, incident investigations and change management, and a form to initiate the change management process; and
3. conduct a complete and thorough investigation to determine the scope of these incidents and ensure the change management forms are completed correctly and the change management process being followed, by spot checking its management forms pursuant to quality assurance steps.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012010893 CIP-004-1 R3 - OVERVIEW

WECC determined that URE failed to update a PRA at least every seven years for one employee (six days late) and failed to conduct a PRA for ten employees prior to granting physical access to all assets at several facilities. The employees had physical and electronic access to CCAs that included workstations and servers and all assets at these facilities. Eight of the employees in scope also had electronic access to ESPs.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The devices in scope are equipped with logging and monitoring controls and are located within secure facilities. The employees in scope received cyber security training and did require access to the CCAs. Finally, all employees in scope were employed in good standing by URE and were granted access following completion of their PRAs.

WECC determined the duration of the violation to be from thirty days after the Standard became mandatory and enforceable, through when URE completed the employees' PRAs.

URE submitted its Mitigation Plan designated WECCMIT008115-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. obtain confirmation that the PRAs were completed;
2. change its practice and no longer accept certification letters as PRA evidence—instead requiring a copy of the background investigation; and
3. reinforce practice through communications from management to key staff members.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012363 CIP-004-2 R4 - OVERVIEW

WECC determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs. Specifically, for approximately a year and a half, URE failed to ensure the performance of quarterly reviews of authorized physical and electronic access to CCAs. In addition, URE did not revoke or update access to its CCAs within seven calendar days for six individuals who no longer required such access.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. While it did not update the access list, URE had manually updated the electronic access for the individuals in the control systems' active directory to reflect new and revoked job responsibilities. Accordingly, the six individuals no longer had electronic or physical access rights to CCAs located within the facilities in scope. Also, the facilities in scope utilize security guards with continuous monitoring and logging, and only qualified and trained personnel with key cards can access these facilities.

WECC determined the duration of the violation to be from eight days after access was first revoked, through when URE updated its access list.

URE submitted its Mitigation Plan designated WECCMIT010178 to address the referenced violations. URE's Mitigation Plan required URE to:

1. submit an access order request to include the affected employee;
2. update the master electronic access list to include the employee's access rights;
3. revise its department procedure relating to CIP-004 R3; and
4. develop stronger controls within that procedure to ensure that information used to perform the 90-day reviews is accurate, and that the electronic access list is updated within seven calendar days of a change. The revised procedure added the following controls:
    a. mandatory use of the access order system for approving and revoking access to NERC CIP facility and CCA;
    b. independent review of the quarterly report;
    c. complete weekly reviews of the electronic access list; and
    d. complete the access worksheet for all access authorizations and revocations.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012357 CIP-005-1 R1 - OVERVIEW

WECC determined that URE failed to identify a router as an access point to the ESP as required by R1.1 and did not provide the protective measures as outlined in R1.5 to the router and a network-monitoring device. The router is an access point to a data link workstation used to provide real-time operating status to a URE facility. The network-monitoring device functions as a data archival unit and handles alerting as an EACM device.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Only four individuals had electronic access to the router, which URE protected with a non-default password and located within a PSP to which only personnel with approved PRAs and cyber security training had access. In addition, URE protected the network-monitoring device with a defense-in-depth architecture of administrative, physical, and logical cybersecurity controls including physical security mechanisms with guards, special locks, and closed-circuit television (CCTV). Finally, URE implemented logical perimeter and internal cyber security controls, including firewalls, vulnerability scanning tools, and a security and events management system that would immediately identify and alert URE technicians of any unusual event or abnormal behavior.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE updated its related documentation and afforded CIP-005 R1.5 protections.

URE submitted its Mitigation Plan designated WECCMIT010576-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. test the access point to make sure all required controls were in place and functional. Upon successful completion of the testing, URE implemented the access point into the production environment and updated the ESP list, plan, and diagram accordingly;
2. conduct complete due diligence of its ESPs to assure it had accounted for all access points. As a result of this effort, URE was able to merge ESPs;
3. replace the original EACM with new hardware and software, tested the controls, put the device into production, added the device to its asset list and categorized it as an EACM, and updated the network topology and ESP diagrams; and
4. institute all required controls for the firewall manager.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012459 CIP-005-3 R4 - OVERVIEW

WECC determined that URE could not demonstrate that it performed an adequate Cyber Vulnerability Assessment (CVA) of its ESP access points for three calendar years. URE's annual CVA process utilized a random sampling of Critical Asset sites and a sample of associated Cyber Assets contained at the selected sites.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE did secure its access points within PSPs. In addition, URE implemented technical and procedural controls that limited access via these access points. Finally, URE monitors all ESP access and has implemented defense-in-depth architecture of administrative, physical, and logical cyber security controls, including physical security mechanisms with guards, special locks, firewalls, and CCTV.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE performed a CVA of its electronic access points.

URE submitted its Mitigation Plan designated WECCMIT010568 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets, including EACM and PACS, and document any discrepancies for remediation; and
2. complete its CVA on all Cyber Assets, EACM devices, and PACS.

URE certified that its Mitigation Plan was completed.

WECC2013012465 CIP-006-3c R1, R1.1 - OVERVIEW

WECC determined that URE failed to ensure certain CCAs within an ESP also reside within an identified PSP. The devices were laptop computers that did not reside within an identified PSP and did not have any evidence of alternative measures to control physical access to the devices. The laptops are configuration devices for control systems. The technicians can use the laptops to connect to the devices and provide system programmability to reduce configuration times.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because the violation encompasses all of URE's PSPs and unauthorized access could have been used to harm the operation of the generation facilities. The risk was mitigated because URE continuously monitors all ESP access and has implemented physical security mechanisms with guards, special locks, firewalls, and CCTV. In the event one of the laptops was compromised, electronic monitoring would provide for immediate notification to personnel responsible for response.

WECC determined the duration of the violation to be from the date URE completed the mitigation activities for a prior noncompliance, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010578 to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the original identified devices from NERC CIP scope and retired to the test environment;
2. update documentation and perform data destruction on the devices;
3. add new desktops to the relevant control centers for configuration purposes; and
4. update the documentation to reflect the new desktops.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012466 CIP-006-3a R2, R2.2 - OVERVIEW

WECC determined that URE failed to identify seven workstations and one server used to authorize access to the PSPs as part of the PACS and failed to afford the PACS devices the protections identified in the Standard. Specifically, URE failed to provide the following protections: 1) the workstations were not segregated from the corporate network and run client software that allows them to communicate with the server in order to authorize physical access to the PSPs; 2) URE did not enable strong technical controls when accessing the PACS server or the PACS network as required by CIP-005 R2.4; 3) URE only required a username and password to access the PACS server from the corporate network; 4) URE failed to implement one or more components of a policy for managing the use of shared accounts that limits access to only those with authorization, an audit trail of account use, and steps for securing the account in the event of personnel change, as required by CIP-007 R5; and 5) URE failed to manage certain shared accounts and afford the shared accounts the protections outlined in CIP-007 R5.2.3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices physically reside within the PSP they were responsible for protecting, thereby receiving continuous physical and electronic monitoring and alarming. The PACS network resides behind the corporate firewall, which URE configured to restrict, monitor, and alert upon suspected malicious activity. Any URE employee that receives access to a shared account must first meet an appropriate business need, obtain approval from an authorized approver, and receive a PRA and mandatory NERC CIP training. Finally, URE reviews individual access to shared accounts quarterly and at any time it revokes access, to ensure shared accounts limit access to only those who are authorized.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010577-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. retire the existing PACS and replace with a new PACS in a separate network that does not provide for external, interactive access;
2. enroll the shared accounts in a system enabling URE to maintain audit trails for personnel having access to those shared accounts;
3. submit required TFEs, which have been approved by WECC; and
4. remove all interactive, external access to the relevant servers and installed devices.

WECC2014013599 CIP-007-1 R8 - OVERVIEW

WECC determined that URE failed to perform a CVA on all Cyber Assets within the ESPs at least annually. URE used port scans for a subset of devices and determined there was no need to scan each device since the un-scanned devices were configured identically to the scanned devices. Consequently, URE could not demonstrate that it performed an adequate CVA of all of its Cyber Assets within its ESPs for four calendar years.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because URE may have been unaware of vulnerabilities on the un-scanned devices, such as default or unauthorized accounts. URE also may have been unaware of unauthorized ports and services existing on un-scanned devices.

The risk was mitigated because URE performed a CVA of a sample set of devices and applied any necessary remediation activities to all like devices. URE also performed quarterly log reviews and

would have been alerted to any suspicious activity. In addition, URE performed port comparisons and would have implemented its incident response if it had encountered any unauthorized accounts or ports and services. Also, where technically feasible, all of URE's devices had antivirus installed. Finally, URE had firewalls at the perimeters of its ESPs that are configured to deny by default, which assists in preventing an attacker's ability to enter URE's network.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010952 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure's assessment methodology to compare documented baseline ports and services configurations to then-running ports and services configurations for all Cyber Assets;
2. document any discrepancies for remediation; and
3. conduct a CVA on all Cyber Assets pursuant to Standard CIP-007-1 R8.

URE certified that its Mitigation Plan was completed.

WECC2013012460 CIP-007-3a R8 - OVERVIEW

WECC determined that URE failed to perform a CVA on all Cyber Assets within the ESPs at least annually. URE's annual CVA process utilized random sampling of Critical Asset sites and a sample of associated Cyber Assets contained at the selected sites. Consequently, URE could not demonstrate that it performed an adequate CVA of its Cyber Assets within all of its ESPs for three calendar years.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was increased because the violation applied to all of URE's Cyber Assets within ESPs for three years. The risk was mitigated because URE secured its devices utilizing access to ESPs within PSPs. In addition, URE had technical and procedural controls in place that limited access via these Cyber Assets during the violation period and monitors all ESP access. Finally, URE has implemented a defense-in-depth architecture of administrative, physical, and logical cyber security controls including physical security mechanisms with guards, special locks, firewalls, and CCTV.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010179 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets, including EACM devices and PACS, and documenting and discrepancies for remediation; and
2. conduct its next CVA on all Cyber Assets, EACM devices, and PACS pursuant to the standard.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred sixty thousand dollars ($160,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations, which WECC considered a mitigating factor;
3. WECC considered the self-reporting of CIP-004-1 R3 as a mitigating factor in penalty determination;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations WECC2013012102, WECC2013012363, WECC2013012466, and WECC2012010893 posed a minimal risk but did not pose a serious or substantial risk to the reliability of the BPS and violations WECC2013012387, WECC2013012357, WECC2013012459, WECC2013012465, WECC2013012460, and WECC2014013599 posed a moderate risk; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred sixty thousand dollars ($160,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

The NERC BOTCC determined that the assessed penalty of one hundred sixty thousand dollars ($160,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director,
Enforcement Processing
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and Deputy
General Counsel
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

November 30, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) submits this Notice of Penalty[1] regarding Unidentified Registered Entity (URE). This Notice of Penalty provides information and details regarding the nature and resolution of the violations,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) issued a Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) to resolve all outstanding issues arising from WECC's determination and findings of the violations of NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

NERC is filing this Notice of Penalty with the Commission based on information from WECC. URE does not contest the violations or the proposed two hundred and five thousand dollar ($205,000) penalty assessment.

Accordingly, NERC is filing the violations in this Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the NOCV issued by WECC. This Notice of Penalty and the NOCV provide the details of the findings and basis for the penalty. This Notice of Penalty filing contains the NERC Board of Trustees Compliance Committee's (NERC BOTCC) basis for approval of the NOCV.

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2014013523	CIP-002-3	R3	High/ High	SC	$205,000
WECC2014014131	CIP-005-3a	R1	Medium/ Severe	SR	
WECC2014013524	CIP-005-3a	R2	Medium/ Severe	SC	
WECC2014014129	CIP-005-3a	R4	Medium/ Severe	SR	
WECC2014013525	CIP-007-3a	R1	Medium/ Severe	SC	
WECC2014014130	CIP-007-3a	R8	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2014013526	CIP-007-3a	R9	Lower/ High	SC	$205,000

WECC2014013523 CIP-002-3 R3- OVERVIEW

WECC determined that URE failed to identify a communications multiplexer and protective relay as Critical Cyber Assets (CCAs) when it added the devices to its Electronic Security Perimeter (ESP) as required by CIP-002-3 R3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE failed to identify two devices as CCAs, the two devices were located within Physical Security Perimeters (PSP) and the ESP. Physical and electronic access to the devices was monitored and restricted to authorized personnel who had background checks and training. The devices were located in protected networks with hardened boundary devices that only allowed traffic from specific IP addresses and ports. URE monitored the communications multiplexer and likely would have been alerted to a loss of communication with the substation. URE conducts annual Cyber Vulnerability Assessments (CVAs) that include a step for network device discovery.

WECC determined the duration of the violation to be from when URE technicians connected the two devices to the ESP, through when URE disconnected both devices from the network.

URE submitted its Mitigation Plan designated WECCMIT011129 to address the referenced violations. URE's Mitigation Plan required URE to:

1. unplug the communications multiplexer from the network;
2. remove access to the protective relay from the firewall and unplug the device;
3. create a new Cyber Asset request form to document proper device identification, ESP, connectivity (IP address), device location, and serial number with post-change validation; and
4. provide training to all construction and engineering groups covering CIP requirements as they apply to each group specifically, including the use of the newly developed forms.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE completed all mitigation activities.

WECC2014014131 CIP-005-3a R1- OVERVIEW

WECC determined that URE failed to identify six access points to the ESP that included any externally connected communication end point terminating at any device within the ESP as required by CIP-005-3a R1.1. URE also failed to afford Cyber Assets used in the access control and/or monitoring of the ESP the protective measures specified in CIP-005-3a R1.5.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to identify six devices as access points, the devices in scope are protected by a firewall with strong access controls for all traffic entering the ESP from external networks. The access controls include two-factor authentication. As a result, individuals require username and passwords and a token in order to access URE's network. URE's architecture requires all traffic entering into the separate virtual local area networks (VLANs) connected to the devices first to pass through the firewall and meet the explicit rules on the access point. These measures reduce the risk of successful VLAN hopping necessary to gain unauthorized access using the six devices in scope.

URE also implemented an intrusion prevention system (IPS) over the energy management system (EMS). The EMS IPS scans EMS traffic for known attack signatures and prevents any known attack signatures that are found. The IPS is designed to identify malware used to compromise the EMS supervisory control and data acquisition (SCADA) devices. URE also implemented an intrusion detection system (IDS) for the EMS and other ESPs on the network. The IDS scans traffic on the ESPs and was designed to detect a breach of the network.

WECC determined the duration of the violation to be from the date the Reliability Standard became mandatory and enforceable through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011659 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document the configuration of the open ports and services on the three electronic access control and monitoring (EACM) devices;
2. fix the script and modify procedures to verify passwords were successfully changed after the script is run;
3. manually change passwords for all six devices in scope;
4. train all information technology security staff members on new procedure;
5. fix internal process to verify script is working;

6. modify CVA processes and procedures to ensure all steps were completed correctly by all groups; and
7. provide training to all personnel involved in performing CVAs as well as those responsible for reviewing CVA results.

WECC2014013524 CIP-005-3a R2- OVERVIEW

WECC determined that URE failed to use an access control model where explicit permissions were specified, and failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP as required by CIP-005-3a R2.1 and R2.2.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to use an access control model where explicit permissions were specified and failed to enable only required ports and services, URE implemented restrictive boundary security controls that had a limited set of IP addresses and services in scope. This control limited the unnecessary vectors a malicious user could attempt to use. URE also implemented strong username and passwords, malicious software prevention tools, and logical monitoring of event logs and access attempts. This control reduced the likelihood that a malicious user could gain access to devices once inside the ESP. URE also implemented alerts on the remote terminal units (RTUs). This control would likely notify URE's control center personnel if a device's connection were lost. Finally, URE also conducted annual CVAs to verify the posture of devices.

WECC determined the duration of the violation to be from when URE put its new EMS into production and did not ensure an unnecessary service was disabled at one ESP access point, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011128 to address the referenced violations. URE's Mitigation Plan required URE to:

1. correct the firewall rules to prevent unauthorized access;
2. complete a full review of existing profiles of business areas for ports and services to determine that ports are accurately and clearly documented; and
3. make additional improvements to the process and training of personnel that will be included in the CIP Version 5 implementation plan.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014129 CIP-005-3a R4- OVERVIEW

WECC determined that for two calendar years, URE failed to include a review during its Cyber Vulnerability Assessment (CVA) to ensure it had enabled only ports and services necessary for operations at the access points and URE failed to document the ports and services in the CVA results and action plan as required by CIP-005 R4.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented preventive controls to address vulnerabilities. These preventive controls included an IPS to scan for and block known attack packet signatures. URE also implemented an antivirus designed to identify and stop malware in the attack packet. The second layer of URE's EMS, the switches, does not support the same port the firewall rule enabled. As a result, the switches would not allow a potential attack to move from the firewalls to the SCADA devices using the port enabled by the firewall rule. URE also implemented detective controls. URE implemented IDS to scan the system for known attack signatures. URE also uses a security information and event management to detect malicious activity and alert appropriate personnel of malicious activity.

WECC determined the duration of the violation to be from when URE first failed to verify in its CVAs that only open ports and services required for operations were enabled, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011445 to address the referenced violations. URE's Mitigation Plan required URE to:

1. modify the existing access point rules to correct the identified issues; and
2. complete the CVA for the EMS and substation access points in order to validate corrections were made.

WECC2014013525 CIP-007-3a R1- OVERVIEW

WECC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls as required by CIP-007-3a R1.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS.

Although URE failed to test firmware upgrades applied to its devices and failed to test additional devices prior to installation, all of the devices were located within PSP. URE limited physical access to

appropriately authorized personnel. All of the devices were installed in an ESP, and URE limited logical access to appropriately authorized personnel. The devices were logically protected by an access point that restricts ports and services. The ESP also logged and monitored malicious activity and likely would have detected abnormal activity on the devices. The relays in scope were located in protected networks with hardened boundary devices and only allowed traffic from specific IP addresses and ports. URE implemented alerts on the RTUs in scope that likely would have notified URE personnel if a link were broken or lost. URE conducted annual CVAs to verify the security posture of the devices in scope. URE also implemented a process to review previous changes made and verify testing was conducted on those changes.

WECC determined the duration of the violation to be from when URE upgraded firmware on devices within the ESP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011127 to address the referenced violations. URE's Mitigation Plan required URE to:

1. compile the devices and associated information in a single list that includes the name of the device (and previous name which will be found in evidence if the name of the device changed), device class, critical asset, IP address, and Technical Feasibility Exceptions;
2. confirm that the upgrade did not change the existing configuration information for the devices beyond version information;
3. perform the validation as part of the CVA; and
4. provide evidence of the validation of the shared accounts and password settings.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE completed all mitigation activities.

WECC2014014130 CIP-007-3a R8- OVERVIEW

WECC determined that URE failed to perform a CVA of all Cyber Assets within the ESP during two calendar years as required by CIP-007-3a R8.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to perform a CVA for the eight switches, URE did implement preventive and compensating controls. URE implemented an IPS designed to scan network traffic for known attack signatures and discover and block malware attacks on the switches. URE also implemented an IDS designed to scan network traffic for known attack patterns and signatures and detect an attacker intruding on the system. URE deployed an antivirus to scan and block attack signatures and malware.

In addition, URE also implemented defense in depth with multiple firewalls between the switches in scope and the border of the network. The defense in depth would require a potential attacker to bypass all layers of the firewall in order to attempt to exploit the switches. URE also used two-factor authentication on its EMS devices, reducing the likelihood of a potential attacker comprising a device.

WECC determined the duration of the violation to be from when URE first failed to perform the CVA of all Cyber Assets within the ESP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011294 to address the referenced violations. URE's Mitigation Plan required URE to perform a CVA on the EMS network switches.

URE certified Mitigation Plan completion, and WECC verified that URE had completed all mitigation activities.

WECC2014013526 CIP-007-3a R9- OVERVIEW

WECC determined that URE failed to ensure that changes resulting from modifications to the systems or controls were documented within 30 calendar days of the change being completed as required by CIP-007-3a R9.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS.

Although URE failed to provide complete test results within 30 calendar days of when the devices were connected to the ESPs, all of the devices were located within PSPs. URE limited physical access to appropriately authorized personnel. All of the devices were installed in an ESP, and URE limited logical access to appropriately authorized personnel. The devices were logically protected by an access point that restricts ports and services. The ESP also logged and monitored malicious activity and likely would have detected abnormal activity on the devices. The relays in scope were located in protected networks with hardened boundary devices and only allowed traffic from specific IP addresses and ports. URE implemented alerts on the RTUs in scope that likely would have notified URE personnel if a link were broken or lost. URE conducted annual CVAs to verify the security posture of the devices in scope. URE also implemented a process to review previous changes made and verify testing was conducted on those changes.

WECC determined the duration of the violation to be from 31 calendar days after URE first made changes resulting from modifications to the systems or controls, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011295 to address the referenced violations. URE's Mitigation Plan required URE to perform a CVA and use the results to confirm that the baseline configurations were correct and unchanged.

URE certified that it completed its Mitigation Plan, and WECC verified that URE completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the NOCV, WECC has assessed a penalty of two hundred and five thousand dollars ($205,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered the instant violations as repeat noncompliance of NERC Reliability Standards and determined the compliance history should serve as an aggravating factor;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE did not receive mitigating credit for self-reporting because the Self-Reports were submitted after receiving notice of an upcoming Compliance Audit;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of WECC2014013523, WECC2014014131, WECC2014013524, WECC2014014129, and WECC2014014130 posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations of WECC2014013525 and WECC2014013526 posed a moderate and not serious or substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that the penalty amount of two hundred and five thousand dollars ($205,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the NOCV and supporting documentation on November 3, 2015 and approved the NOCV. In approving the NOCV, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

The NERC BOTCC approved the NOCV and believes that the assessed penalty of two hundred and five thousand dollars ($205,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

November 30, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2], in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of NERC Reliability Standards. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred thousand dollars ($200,000), in addition to other remedies and

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2013012023	CIP-003-3	R5	Lower/ Severe	SC	$200,000
WECC2014013497	CIP-003-3	R6	Lower/ Moderate	SC	
WECC2012011467	CIP-005-1	R1	Medium/ Severe	SR	
WECC2013012367	CIP-005-3a	R5	Lower/ Severe	SC	
WECC2013012368	CIP-006-1	R1	Medium/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2013012025	CIP-006-3c	R4	Medium/ Severe	SC	$200,000
WECC2012011598	CIP-006-3c	R5	Medium/ Severe	SR	
WECC2014013498	CIP-007-3a	R1	Medium/ Severe	SC	
WECC2014013658	CIP-007-3a	R2	Medium/ Severe	CA	
WECC2013012369	CIP-007-3a	R3	Lower/ Severe	SC	
WECC2012011599	CIP-007-1	R5	Medium/ Severe	SR	
WECC2014013499	CIP-007-3a	R5	Medium/ Severe	SC	
WECC2013012370	CIP-007-3a	R9	Lower/ High	SC	
WECC2014013500	CIP-007-3a	R9	Lower/ High	SC	
WECC2013012029	CIP-009-1	R1	Medium/ Severe	SC	

WECC2013012023 CIP-003-3 R5 - OVERVIEW

WECC determined that URE did not verify annually the list of personnel responsible for authorizing access to protected information. WECC determined the violation included seven individuals working within URE's various departments.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). As a result of URE's failure, unauthorized individuals may have had access to sensitive information. The potential risks associated with this violation were, however, limited due to URE's additional procedures. URE completed a review and promptly remediated the violation. URE has a limited number of individuals authorized to grant access to protected information; thus, any attempts by others to grant access to protected information would have been promptly discovered. Finally, when URE verified the list, the list remained the same and no employee was removed or added.

WECC determined the duration of the violation was one calendar year and resolved when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009349 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. update the CIP-003 access procedure;
2. review the access list and record it in the review history section of the documentation;
3. implement a review form to record future annual reviews; and
4. schedule a calendar reminder to begin the review and to submit the appropriate documentation no later than December 30th of each year.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013497 CIP-003-3 R6 - OVERVIEW

WECC determined URE upgraded firmware and that URE failed to implement its Change Control and configuration management program across a subset of devices within URE's critical facilities while upgrading the firmware.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Because the firmware upgrade was not tested prior to installation, the firmware patch could have enabled ports and services or created unauthorized user accounts. Although URE failed to perform security testing prior to installing firmware upgrades, URE did implement preventive controls. Specifically, all of the relays in scope are located within Physical Security Perimeters (PSPs) and Electronic Security Perimeters (ESPs). URE monitors physical and logical access to the PSPs and

ESPs. URE also restricts access to authorized personnel with background checks and training on proper handling of the devices. URE placed the relays in protected networks with hardened boundary devices.

WECC determined the duration of the violation was from the time URE upgraded the firmware, to when URE followed its Change Authorization and Configuration Management protocol for the devices in scope.

URE submitted its Mitigation Plan designated WECCMIT011627 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. grant change authorization for the devices;
2. perform all security testing pursuant to CIP-007-3 R1;
3. implement job plan templates that include a notice to complete CIP-related tasks as part of computer-based work orders;
4. document and implement a process for adding new CIP equipment as it relates to system planning and automation; and
5. provide training on the new job plan and process document to applicable employees.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011467 CIP-005-1 R1- OVERVIEW

URE reported that it conducted a Cyber Vulnerability Assessment (CVA) and identified devices that should have been classified and protected as non-critical Cyber Assets.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE did not meet the requirements of this Standard, URE did minimize the potential risks associated with this violation. Specifically, URE ensured that all devices involved in the violation were physically and electronically protected from unauthorized access 24 hours a day 7 days a week. Additionally, all URE personnel with access to the devices had undergone personnel risk assessments (PRAs) and had received CIP training. Finally, any actual access to the devices was monitored 24 hours a day 7 days a week.

WECC determined the duration of the violation to be from when URE was required to demonstrate compliance with this Standard through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009590-2 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. remove the two IP connections for the management interfaces of the taps from the ESP;
2. relocate the connections to the unregulated quality assurance system;
3. provide the necessary protections to meet compliance and provide all relevant evidence. URE updated the CIP asset list to reflect the Cyber Assets' new designation, which is as both a Critical Cyber Asset (CCA) and an Electronic Access Control and Monitoring device (EACM);
4. submit a Technical Feasibility Exception request for the devices;
5. upgrade those authentication manager servers to the latest platform and perform a CVA on them prior to production; and
6. update the security operations recovery plan to include processes and procedures for the backup and storage of information required to successfully restore the EACM devices.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012367 CIP-005-3a R5 - OVERVIEW

WECC determined that URE failed to review, maintain, and update all documentation required by CIP-005-3a. WECC also determined that URE failed to update, within 90 calendar days, its ESP diagram when it decommissioned certain devices.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure increased the likelihood that changes in its network would go unnoticed and improper information about the network would be communicated to URE employees and contractors. The potential risks associated with this violation however, were limited due to URE's additional action of reviewing documentation in the years before and after the failure.

WECC determined the duration of the violation to be from when URE failed to review and update its documentation through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009383 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review documents and procedures referenced in Standard CIP-005-3;

2. update CIP-005 R5 documentation review procedure;
3. update the ESP diagram to remove the decommissioned asset; and
4. update the CIP master asset List to remove the decommissioned asset.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012368 CIP-006-1 R1 - OVERVIEW

WECC determined URE failed to provide node controllers the protections of CIP-007 R1, R2, R4, R5, and R9. Additionally, WECC determined URE failed to perform an annual exercise of its workstation recovery plan and failed to annually test its workstation backup media as required by CIP-009 R2 and R5. Furthermore, WECC determined URE failed to document its patch assessments for certain servers.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE failed to provide certain protections required by the Standard, URE did limit the potential risks associated with the violation by employing different compensating measures. Specifically, for the node controllers involved in the violation, URE protected the devices from unauthorized access, and all personnel with access were authorized and had undergone PRAs and received CIP training. Additionally, URE tested and deployed available patches to the devices in scope.

WECC determined the duration of the violation was from the date the Standard became mandatory and enforceable, to when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT009349 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. schedule work with the application service vendors to complete full implementation of CIP controls;
2. perform the review of the recovery plan for the workstation;
3. perform the testing on the workstation backup media;
4. create an annual assessment calendar; and
5. provide training to all relevant group members.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012025 CIP-006-3c R4 - OVERVIEW

URE self-reported that at a substation PSP, on seven occasions, the access security badge reader was bypassed and the magnetic lock failed to operate as intended.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure created opportunities for individuals without authorization to access URE's PSPs and the CCAs located within the PSP. The potential risks associated with this violation, were however, limited due to URE's additional measures in place during the pendency of the violation. Specifically, the PSP in scope had alarm monitoring and a separate third-party monitoring alarm system. Additionally, the PSP is surrounded by a barbed wire fence and has a control gate with an alarm attached. Furthermore, the CCAs located within the PSP are fully monitored, and access is logged 24 hours a day 7 days a week.

WECC determined the duration of the violation to be from the first date the magnetic locks failed to open, to the last date the magnetic locks failed to operate.

URE submitted its Mitigation Plan designated WECCMIT011616 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. provide additional training to substation operations personnel regarding physical security at CIP substations; and
2. strengthen its overall approach to CIP security at the substations by designating security officers to regularly monitor alarms from the security system.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011598 CIP-006-3c R5 - OVERVIEW

URE reported that at a substation PSP, the security management system (SMS) reported a communication failure at its card readers. Because of the SMS outage, the substation PSP card readers were locked down and were not monitoring during the outage. URE reported that the outage continued for three days.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure created opportunities for individuals without authorization to access PSPs and the CCAs located within the PSP. The potential risks associated with this violation were, however, limited due to URE's additional measures in place during the pendency of the violation. Specifically, the PSP in scope had alarm monitoring and a separate third-party monitoring alarm system. Additionally, the PSP is surrounded by a barbed wire fence and has a control gate with an alarm attached. Furthermore, the CCAs located within the PSP are fully monitored, and access is logged 24 hours a day 7 days a week.

WECC determined the duration of the violation was from the date when the substation PSP experienced an SMS outage and monitoring failure, to when URE reestablished monitoring capability at the substation.

URE submitted its Mitigation Plan designated WECCMIT009373 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review existing CIP documentation;
2. update corporate security procedures to include sufficient detailed instructions about how to respond to outages when the outage duration is longer than the 10-minute threshold for rebooting the system;
3. develop a new process and procedure that defines how the system will be used to address CIP-006 R5 as a secondary monitoring mechanism during outage situations; and
4. train personnel on the new procedures.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013498 CIP-007-3a R1 - OVERVIEW

WECC determined the URE implemented a firmware upgrade on relays at Critical Asset facilities. WECC determined the relays were not flagged as CIP-protected devices. Therefore, WECC determined URE did not conduct security testing prior to installing the firmware upgrade to ensure the firmware upgrades did not adversely affect existing cyber security controls.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In this instance, URE failed to perform security testing prior to installing firmware upgrades on protective relays. This could negatively impact the existing cyber security controls on

these relays. Although URE failed to perform security testing prior to installing firmware upgrades, URE did implement detective controls. Specifically, all relays in scope are located within PSPs and ESPs. URE monitors physical and logical access to the PSPs and ESPs. URE also restricts access to authorized personnel with background checks and training on proper handling of the devices. URE placed the relays in protected networks with hardened devices. As a result, the relays were logically protected to allow traffic from only specific IP addresses and ports. These controls limit the vectors malicious personnel could use when attempting to compromise the devices.

URE also implemented detective controls. Specifically, URE had a control and monitoring network that would monitor and alarm if it detected a relay or breaker misoperation. URE implemented additional compensating controls. Specifically, prior to installing the patch in production, URE conducted functional testing in a test environment to test the effect of the change on the relays. By doing so, URE tested the patch to verify it would not break or damage the relay during installation.

WECC determined the duration of the violation was from the date URE upgraded the firmware, to when URE conducted post-testing to ensure there was no compromise of existing security controls.

To mitigate this violation, URE conducted post-testing to ensure there was no compromise of existing security controls. Based on the voluntary corrective actions taken by URE, WECC determined URE is not required to submit a Mitigation Plan for this violation.

WECC2014013658 CIP-007-3a R2 - OVERVIEW

URE directed WECC to use ports and services lists created for the annual CVA as baselines for its assessment during the Compliance Audit. WECC determined certain of these lists provided by URE lacked business justifications for the open ports and services. WECC also determined certain of URE's ports and services process documentation did not contain complete or updated lists of approved ports and services.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Failing to enable only ports and services required for normal and emergency operations could allow attackers to gain unauthorized access to the devices in scope. However, URE implemented certain compensating measures, including preventive and detective controls.

Specifically, all of the Cyber Assets reside behind electronic access points which restrict logical access to only authorized users. Additionally, all Cyber Assets physically reside within a PSP and are protected against unauthorized physical access. URE also employs intrusion detection, prevention, and antivirus

tools to detect and deter unauthorized access. These preventive and detective controls may prevent unauthorized individuals from gaining access or causing harm to the devices in scope

WECC determined the duration of the violation was from the first day of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011627 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review its ports and services documentation to ensure that it is updated to reflect the current configuration of all CIP Cyber Assets; and
2. ensure that an appropriate business justification is identified for all open ports and services.

URE certified that its Mitigation Plan was completed.

WECC2013012369 CIP-007-3a R3 - OVERVIEW

WECC determined that URE became aware of new security patches or upgrades available for six EMS servers. WECC determined URE failed to adequately document the assessments of the applicability of security patches and security upgrades within 30 calendar days of availability in violation of CIP-007-3a R3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to properly document its assessment security patches security upgrades increased the likelihood that its Cyber Assets may not be properly protected from potential cyber-attacks. The risks posed by URE's noncompliance were limited due to URE's additional protections. Specifically, URE assessed the security patches but failed to document that assessment as required by the Standard, thus the devices were up-to-date with appropriate protections. In addition, the EMS servers involved in the violation reside within a designated ESP. The ESP is monitored 24 hours a day, 7 days a week and produces active logs of activities that occur within the ESP.

WECC determined the duration of the violation was 30 calendar days after the release of the security patches, to when URE completed the assessment of the security patches.

URE submitted its Mitigation Plan designated WECCMIT009384 to address the referenced violations.

URE's Mitigation Plan required URE to update its procedures for its EMS and Windows patch assessment spreadsheet and assess patches that were missed.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2012011599 CIP-007-1 R5 - OVERVIEW

URE reported that it had one shared account, with access to EMS servers, which did not receive annual password changes. URE stated that the shared account was an emergency account and that it had never been used. URE also reported that devices at different locations did not have strong second-level passwords. URE reported that the second-level passwords had been changed from the factory default, but the passwords were not of sufficient strength to meet the requirements of CIP-007-1 R5.3.2.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to establish proper passwords and ensure that passwords are changed annually resulted in a situation where unauthorized access to the Cyber Assets could go unnoticed and unchecked. The potential risk associated with the violation was reduced due to URE's compensating measures.

URE had a strong password for the one shared account that was not changed annually. Additionally, all employees who had access to the one shared account had undergone PRAs and had comprehensive CIP training. Moreover, the EMS servers that were accessible from the one shared account generate activity logs that are actively monitored to ensure that only authorized individuals access the servers. URE also limited the potential risks associated with the devices that did not have strong second-level passwords. URE reported that each of the devices involved resides within a PSP and an ESP. Additionally, the devices were only accessible by certain personnel, each of whom had undergone PRAs and had received comprehensive CIP training. Moreover, the first-level passwords were strong passwords that met the complexity and length requirements of CIP-007-1 R5.

WECC determined the duration of the violation was from the date URE first failed to have strong second-level passwords on the devices, to when URE changed the second-level passwords on the devices.

URE submitted its Mitigation Plan designated WECCMIT009276-1 to address the referenced violation.

URE's Mitigation Plan required URE to:

1. change the emergency shared account password;

2. change the configuration of this account so that if the password is not changed within 90 days of use, the account password will automatically expire and require a reset prior to use; and
3. change the second-level passwords for the devices to strong passwords.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013499 CIP-007-3a R5 - OVERVIEW

WECC determined URE failed to change passwords at least annually on certain accounts in violation of CIP-007-3a R5.3.3. WECC determined three accounts had administrator access to the EMS domain workstations, one account had file transfer permissions to and from the open systems interconnection application, and the final account had local user access to the EMS workstations. WECC determined the workstations associated with the accounts are located at URE's system control center and backup control center.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to change passwords at least annually on accounts. Failing to change passwords at least annually on these accounts could allow unauthorized individuals or individuals no longer authorized to have access to the devices in scope. However, in this instance URE had compensating measures and implemented preventive controls. Specifically, access to user accounts is managed through URE's account management tool. The tool ensures that only authorized individuals are granted access to EMS workstations and remote interactive access into the ESP is limited to individuals who require access. In addition, the shared account passwords at issue were known by a limited number of individuals and were not intended for human use.

WECC determined the duration of the violation was one year after URE last changed the passwords through completion of its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011638 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. change the passwords that will be reviewed each quarter by information technology department managers;
2. manage interactive access into the EMS environment account; and
3. remove the account from all CCAs on which it resides.

WECC2013012370 CIP-007-3a R9 - OVERVIEW
WECC determined that URE's departments failed to review CIP-007-3 documentation annually.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to perform an annual review on its CIP-007-3 documentation presented an opportunity where changes to the documents would not have been properly reflected and protections offered to CCA may not have been properly applied or removed. The potential risks associated with this violation were limited due to URE's additional procedures. Specifically, URE had conducted a review of the documentation in the previous year and, upon discovery of the possible violation, immediately conducted a review of its CIP-007-3 documentation.

WECC determined the duration of the violation began when URE failed to conduct the annual review and ended when URE reviewed the CIP-007-3 documentation.

URE submitted its Mitigation Plan designated WECCMIT009386 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. review the access list and record it in the review history section of the documentation;
2. review the documents;
3. update the CIP-007-3a R9 documentation review procedure;
4. create a calendar that lists all assessment activities that need to take place on a monthly, quarterly, and annual basis; and
5. train applicable group members on the new process.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2014013500 CIP-007-3a R9 - OVERVIEW
WECC determined that URE did not review its CIP-007-3 R4 antivirus document annually, in violation of CIP-007-3a R9.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failing to review and update documentation could lead to personnel performing out of date or incorrect processes on the devices in scope. However, URE implemented preventive controls as compensating measures. URE tests significant changes to devices prior to deploying

changes. This would alert URE to any issues prior to the changes affecting the devices in scope. Additionally, URE updated its calendar spreadsheet for tracking the annual procedure reviews.

WECC determined the duration of the violation began when URE failed to review the antivirus document and ended when URE reviewed the antivirus document.

URE submitted its Mitigation Plan designated WECCMIT010931 to address the referenced violations.

URE's Mitigation Plan required URE to review the antivirus for EMS procedure.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

WECC2013012029 CIP-009-1 R1 - OVERVIEW

WECC determined URE failed to conduct one annual review of its EMS recovery plan. As a result, WECC determined URE was in violation of CIP-009-1 R1.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure increased the opportunity for its CCA to be rendered inoperable in the event of an emergency. The potential risks associated with the violation were limited due to additional protections in place during the pendency of the violation. Specifically, the EMS workstations involved in the violation were located within a defined ESP and PSP. Furthermore, URE monitors physical and logical access to the devices 24 hours a day 7 days a week. Finally, URE did have a partial recovery plan in place and had trained its operators on the recovery plan.

WECC determined the duration of the violation was for one calendar year.

URE submitted its Mitigation Plan designated WECCMIT009282-2 to address the referenced violations.

URE's Mitigation Plan required URE to:

1. create a group annual assessment calendar that will list all assessment activities that need to take place on a monthly, quarterly, and annual basis;
2. revise the recovery plan to contain more detail on severity and duration and also include more detail for roles and responsibilities, including which departments to contact, what the role of each department is, and a contact phone number for each department; and
3. train all applicable group members on the new process.

URE certified that its Mitigation Plan was completed, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred thousand dollars ($200,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE self-reported three of the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of WECC2013012023, WECC2014013497, WECC2013012368, WECC2013012367, WECC2013012025, WECC2012011598, WECC2014013498, WECC2014013658, WECC2013012369, WECC2012011599, WECC2014013499, WECC2013012370, and WECC2014013500 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The violations of WECC2014013658, WECC2012011467, and WECC2013012368 posed a moderate risk but did not pose a serious or substantial risk to the reliability of the BPS;
7. URE agreed to implement Reliability Focused Terms;[4]
8. URE sent WECC a letter reporting on URE's successful progress in implementing the Reliability Focused Terms outlined in the Settlement Agreement; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[4] URE committed to the following terms: 1) to strengthen preventive and detective controls to minimize human error associated with the performance of CIP compliance related tasks; 2) to engage an outside consultant to support URE's transition to CIP Version 5 by analyzing URE's CIP controls; 3) to report to WECC on its progress in these efforts by the end of second quarter of 2015; and 4) to complete the work pertaining to the above non-monetary sanctions no later than December 31, 2015.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred thousand dollars ($200,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders, the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred thousand dollars ($200,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[5] *See* 18 C.F.R. § 39.7(d)(4).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net
Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz	Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz
Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
edwin.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

December 30, 2015

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations of CIP Reliability Standards.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred and thirty-five thousand dollars ($235,000), in addition to

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between SPP RE and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	Discovery Method* Date	Penalty Amount
SPP2013013217	CIP-002-3	R3.1	SR	$235,000
SPP2013013218	CIP-003-3	R6	SR	
SPP2013013224	CIP-005-3a	R4.3, R4.5	SR	
SPP2013013225	CIP-006-3a	R2.2	SR	
SPP2013013226	CIP-007-3a	R1.1, R1.2, R1.3	SR	

NERC Violation ID	Standard	Req	Discovery Method* Date	Penalty Amount
SPP2013013227	CIP-007-3a	R2.1	SR	$235,000
SPP2013013231	CIP-007-3a	R6.2, R6.4	SR	
SPP2014013561	CIP-005-3a	R3.2	SC	
SPP2014013565	CIP-007-3a	R3.1, R3.2	SC	
SPP2014013566	CIP-007-3a	R8.4	SC	

SPP2013013217 CIP-002-3- OVERVIEW

SPP RE determined that URE did not maintain a complete list of Critical Cyber Assets (CCAs). URE installed human machine interface client software, which is used to access URE's supervisory control and data acquisition/energy management system (SCADA/EMS) on devices, including workstations, desktops, and laptops, all of which were outside of URE's Electronic Security Perimeter (ESP). URE failed to include these devices on its CCA list as required by CIP-002-3 R3.1.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). This violation presented the risk that the SCADA/EMS could be compromised because the human machine interface client software could allow a direct connection to the production EMS from the devices on which the client software was installed, and these devices were neither identified nor protected as CCAs. The software deployments were installed on devices outside the ESP, including laptops used primarily for after-hours on-call support; virtual workstations used by distribution operators; and desktops in the organization. The software was installed on six desktops inside the ESP that were listed as CCAs, but not afforded CIP protections. The workstations used by the distribution operators were protected by the ESP firewall. Of the 120 users with access via the software, only 22 (18%) had administrative rights for the SCADA/EMS. The 22 users received access based on a business need, completed NERC training (CIP and Operations and Planning), and had current personnel risk assessments (PRA). These users were comprised of EMS and transmission

planning staff. URE maintained strong authentication access controls for the users, such as requiring an appropriate individual username and password, token authorization, and firewall authorization. The remaining users were granted read-only access rights to the EMS.

SPP RE determined the duration of the violation to be from the day after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010511 to address the referenced violations. URE's Mitigation Plan required URE to:

1. conduct an infrastructure and architecture review of its full environment;
2. appropriately classify devices (newly identified and existing) based on its methodology, and modify its master CIP device list;
3. commission newly identified assets according to URE's processes;
4. implement a commissioning process for all existing devices on its master CIP device list;
5. train and provide communications materials to affected personnel on URE's inventory and commissioning processes; and
6. add a quality review step within URE's commissioning process for compliance validation prior to putting an asset in service.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013218 CIP-003-3- OVERVIEW

SPP RE determined that URE did not adhere to its change control and configuration management process. Specifically, URE personnel made changes to an Electronic Access Control and Monitoring System (EACMS) in the production environment, rather than in the test environment. Additionally, an approved change management request was not acquired before patches were installed on four EACMS and a Physical Access Control System (PACS), and group policy settings were made in URE's production environment.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-003 R6 has the potential to compromise the reliable operation of the BPS by exposing CCAs to potential vulnerabilities resulting from application of undocumented change control or configuration management activities. Notwithstanding, URE did have protective measures in places that reduced the risk. For example, all of the affected devices resided within URE's

ESP; URE was logging and monitoring access to these devices for potential security events; and URE's CCAs were protected by firewalls specifically configured to allow only authorized traffic to enter the network, thereby preventing unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights, all of whom had completed CIP training and possessed current personnel risk assessments.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011015 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its change control and management process to include additional steps, i.e., a sign-off checklist, to ensure adherence to the process;
2. implement preventive and detective controls to identify or disable the ability to implement changes to CCAs in other than the test environment; and
3. provide training to all affected staff.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013224 CIP-005-3a - OVERVIEW

SPP RE determined that URE's Cyber Vulnerability Assessments (CVAs) for two calendar years did not include a visual inspection of physical devices to verify that all electronic access points to the ESP were identified (R4.3). Additionally, the CVA results did not include action plans to remediate or mitigate potential vulnerabilities identified by the CVAs (R4.5).

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. When potential cyber security vulnerabilities are left unresolved or unmitigated, they create the opportunity to exploit those vulnerabilities thereby exposing devices to potential cyber attack. Failing to identify all access points to the ESP also increases the risk of cyber attack because such access points may not be afforded adequate security measures. Nevertheless, the CVAs addressed requirements R4.1, R4.2, and R4.4. For example, URE's maintained a document identifying the vulnerability assessment process (R4.1); conducted reviews to verify that only ports and services

required for operations at access points to the ESP were enabled (R4.2); and reviewed controls for default accounts, passwords, and network management community strings (R4.4). URE was logging and monitoring identified access points to its ESP. Additionally, URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unauthorized access to the ESP. Network traffic, at URE's ESP access points, was analyzed for known and suspected malicious activity using a network intrusion detection system. Access to all Cyber Assets inside the ESP was limited to only those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the publication date of the CVA report for the first calendar year, through when the URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010972 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its CVA process to:
    a. require visual inspections of physical devices located within the ESP;
    b. require action plans to remediate or mitigate potential vulnerabilities identified in the CVAs;
2. provide training to all affected staff; and
3. conduct a CVA that included the above revisions to the CVA process.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013225 CIP-006-3a- OVERVIEW

SPP RE determined that URE did not afford all of the protective measures specified in CIP-003-3 R6 and CIP-007-3 R1, R3, R5.3.3, and R6 to some PACS devices.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. By not affording CIP protections to the PACS, the risk existed that the Physical Security Perimeter (PSP) could be compromised. SPP RE determined that no breach of URE's PSP, CCAs, or data resulted from a lack of change control or configuration management of the PACS. URE's Cyber Assets were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also used system logging to analyze network traffic at access points to the ESP for known and suspected

malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010973 to address the referenced violations. URE's Mitigation Plan required URE to:

1. upgrade its servers to provide sustainable support;
2. conduct infrastructure and architecture review of the full system environment;
3. assess all devices using updated classification methodology and appropriately record those on the master CIP device list;
4. commission newly identified assets according to established processes;
5. implement a commissioning process for all CIP-related cyber assets identified or existing on master CIP device list;
6. train applicable personnel and distribute communications materials on its inventory and commissioning processes; and
7. institute a quality review step within its commissioning process for compliance validation prior to assets being placed in service.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013226 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not ensure that significant changes to Cyber Assets within the ESP did not adversely affect existing cyber security controls.

URE did not test multiple significant changes to Cyber Assets within the ESP prior to implementing the changes in the production environment. Additionally, an information technology technician scheduled patching for Cyber Assets in the test environment and mistakenly included a production PACS device in the automated system used for downloading patches. Accordingly, URE failed to ensure that significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007 R1 provides the opportunity for new Cyber Assets within the ESP and significant changes to existing Cyber Assets within the ESP to adversely affect existing cyber security controls. Notwithstanding, URE had implemented security controls test procedures and tested most changes in accordance with such procedures. The identified Cyber Assets were located within a PSP. In addition, all network traffic that was within the ESP was logged and monitored by URE's system log server, which was configured to send alerts to IT personnel had any unusual traffic been suspected. URE's CCAs were protected by a firewall configured to allow only traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. The URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to only those individuals with authorized physical and/or electronic access rights. The URE discovered the violation as part of its Internal Compliance Program review processes.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010971 to address the referenced violations. URE's Mitigation Plan required URE to:

1. enhance its existing cyber security controls test process and institute technical or procedural controls to ensure that testing minimizes the impact to production systems;
2. institute quality assurance steps in its current change management process, including cyber security controls test validation;
3. implement a sign-off check list for the quality assurance steps in the change management process;
4. institute preventive/detective controls to identify or disable the possibility to confuse environments for changes or testing; and
5. deliver training and distribute awareness communications (cyber security controls test and current change management process changes) to applicable staff.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013227 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not include some CCAs in its ports and services control procedure. As a result, URE was unable to ensure that only those ports and services required for normal and emergency operations were enabled.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007-3a R2.1 has the potential to allow the infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations. Although URE had not identified all of it CCAs, it had implemented a process to regularly review ports and services of CCAs. The devices in question were located within an ESP and PSP. In addition, all network traffic within its ESP was logged and monitored by URE's system log server, which was configured to send alerts to IT personnel when any unusual traffic is identified. URE's CCAs were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010478 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a process to establish and maintain a baseline of ports and services and workflow to ensure only those ports and services that are required for normal and emergency operation are enabled;
2. institute preventive or detective controls (i.e., exception reporting, etc.) for ports and services to identify additions or changes;
3. institute preventive/detective controls to identify or disable the possibility to confuse environments for changes or testing; and
4. deliver ports and services training to applicable staff.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2013013231 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not correctly format four automated alerts, which prevented the issuance of automated alerts for detected cyber security incidents. However, during further discussions with URE, SPP RE determined that URE had an additional instance of noncompliance with CIP-007-3a R6.2 and an instance of noncompliance with R6.4.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007 R6 has the potential to allow the compromise of CCAs and other system cyber security events to occur without URE's knowledge. Where automated alerting was not generated because the logs were not sent to the centralized logging server, the logs were retained at the devices. The period that logs were not captured was limited to maintenance outages. URE manually monitored the centralized logging server on a daily basis during business hours for any logging failures (missing logs or invalid formats).

Regarding this instance of noncompliance, URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to Cyber Assets inside the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010477 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop and implement a new process to identify logging and alerting failures;
2. implement an alternative technology to replace the centralized logging server;
3. implement a commissioning process for CIP-related cyber assets to include validation of alerting, capture of electronic logs, and retention of such logs; and
4. provide training to all affected staff.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2014013561 CIP-005-3a - OVERVIEW

SPP RE determined that URE did not monitor all access points to the ESP for attempted or actual unauthorized access, twenty-four hours a day, seven days a week.

URE's satellite clocks were electronic access points (EAPs) located inside URE's ESP. The clocks were used to provide global position system data to establish time values, and were serially connected to URE's EMS data acquisition servers, which were CCAs located in URE's ESP. It was technically infeasible for the clocks to alert for attempts at or actual unauthorized access to the ESP; however, URE failed to file a Technical Feasibility Exception (TFE) with SPP RE.

URE's modem sharing devices were EAPs located inside URE's ESP and communicated with its field Remote Terminal Units (RTUs). It was technically infeasible for these modem sharing devices to alert for attempts at or actual unauthorized access to the ESP; however, URE failed to file a TFE with SPP RE.

During an audit, SPP RE discovered two EACMs/EAP devices and two CCA devices that were continually logging access to the ESP, which were sent to the centralized logging server. However, it was technically infeasible for the server to generate automated alerts for attempts at or actual unauthorized access to the ESP, and URE failed to file a TFE with SPP RE.

As to the above instance of noncompliance, URE was not reviewing or otherwise assessing access logs for attempts at or actual unauthorized access at least every ninety calendar days.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-005-3a R3 provides the opportunity for access attempts or unauthorized access to the ESP to occur without URE's knowledge. Notwithstanding URE's failure to implement the mitigating measures associated with TFEs, URE had implemented a documented process for monitoring and logging access at access points to the ESP. URE's firewalls were configured to allow only electronic traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to all Cyber Assets within the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the date after the completion of the previous audit, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011019 to address the referenced violations. URE's Mitigation Plan required URE to:

1. implement an enhanced commissioning process including TFE identification on CIP-related Cyber Assets;
2. implement tools for monitoring, alerting, and retaining logs for applicable CIP-related Cyber Assets;
3. develop a process to identify and remediate gaps in monitoring or alerting; and
4. deliver training to applicable staff.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2014013565 CIP-007-3a - OVERVIEW

SPP RE determined that URE's centralized logging server was utilized for electronic access control and monitoring of Cyber Assets located within URE's ESP. Available security patches for the centralized logging server were not evaluated, tested, or installed (R3.1), and no compensating measures were applied to mitigate risk exposure (R3.2).

During an audit, SPP RE discovered additional instances of noncompliance with CIP-007-3a R3.1 and R3.2. A security patch for six network switches was not installed (R3.1), and no compensating measures were applied to mitigate risk exposure (R3.2).

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. A violation of CIP-007-3a R3 provides the opportunity for infiltration of unauthorized network traffic into the ESP when security patches and upgrades are not installed on Cyber Assets within the ESP. All network traffic within URE's ESP was logged and monitored by URE's system log server, which is configured to send alerts to IT personnel when any unusual traffic is identified. URE's CCAs were protected by firewalls configured to allow only traffic using specific protocols to enter the network, which prevents unsolicited traffic from passing into the ESP. URE also used a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to CCAs was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the completion date of URE's mitigation plan for previous violations of the same standard and requirement, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT011021 to address the referenced violations. URE's Mitigation Plan required URE to:

1. execute its commissioning process, including TFE identification, for all CIP-related cyber assets identified or existing on the master CIP device list;
2. enhance its patch management processes for consistency in tracking and monitoring applicable patches and compensating measures for CIP related Cyber Assets;
3. integrate patch management processes with change and configuration management processes; and
4. train applicable personnel and provide communication materials on the inventory and commissioning process.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

SPP2014013566 CIP-007-3a - OVERVIEW

SPP RE determined that URE did not include action plans to remediate or mitigate potential vulnerabilities identified in the CVAs for two calendar years.

SPP RE determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Failure to mitigate vulnerabilities identified in the CVA assessment and track the implementation of corrective action plans has the potential to allow vulnerabilities to continue unmitigated. Notwithstanding, URE conducted CVAs in those calendar years that addressed the remainder of the required information prescribed in R8. URE was logging and monitoring Cyber Assets within its ESP. URE maintained firewalls that were configured to allow only electronic traffic using specific protocols to enter the network, which prevented unsolicited traffic from passing into the ESP. URE also utilized a network intrusion detection system to analyze network traffic at access points to the ESP for known and suspected malicious activity. Access to Cyber Assets inside the ESP was limited to those individuals with authorized physical and/or electronic access rights.

SPP RE determined the duration of the violation to be from the publication date of the first CVA Report, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated SPPMIT010929 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its CVA process to require action plans to remediate or mitigate potential vulnerabilities identified in the CVAs;
2. provide training to all affected staff; and
3. conduct a CVA inclusive of the above revisions to the CVA process.

URE certified that it had completed its Mitigation Plan, and SPP RE verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of two hundred and thirty-five thousand dollars ($235,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. SPP RE considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SPP RE considered as a neutral factor in penalty determination;
3. URE self-reported three violations, but did not receive mitigating credit for seven other violations because they were submitted approximately four months prior to a Compliance Audit, which was after receiving notice of the upcoming audit;
4. URE was cooperative throughout the compliance enforcement process;
5. URE did not evidence any attempt to conceal a violation nor the intent to do so;
6. all of the violations posed a moderate but not a serious or substantial risk to the reliability of the BPS; and
7. SPP RE found there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of two hundred and thirty-five thousand dollars ($235,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 16, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred and thirty-five thousand dollars ($235,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Ron Ciesiel* General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 614-3265 (501) 821-8726 – facsimile rciesiel.re@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1672 (501) 821-8726 – facsimile jgertsch.re@spp.org SPP RE File Clerk* Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1681 (501) 821-8726 – facsimile spprefileclerk.re@spp.org	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 28, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations of CIP-002, CIP-003, CIP-004, CIP-005, CIP-006, and CIP-007.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing the violations in this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC201002262	CIP-002-1	R1; R1.2; R1.2.2; R1.2.4	Medium/ Severe	SC	No Penalty
WECC201002354	CIP-002-1	R3; R3.1	High/ Severe	CA	
WECC201002355	CIP-003-1	R1; R1.1; R1.2; R1.3	Medium/ Severe	SR	
WECC201002356	CIP-003-2	R4.3	Medium/ Severe	SR	
WECC2013011670	CIP-003-3	R5	Lower/ Severe	SR	
WECC200801173	CIP-004-1	R2	Lower/ Severe	SR	
WECC200801174	CIP-004-1	R3	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC2014014185	CIP-004-3a	R3	Medium/ Severe	SR	No Penalty
WECC201002280	CIP-004-1	R3; R3.2	Medium/ High	SR	
WECC200801175	CIP-004-1	R4	Lower/ Lower	SR	
WECC201002381	CIP-005-1	R1	Medium/ Severe	SR	
WECC201102851	CIP-005-1	R1; R1.4	Medium/ Severe	SR	
WECC200901633	CIP-005-1	R1; R1.5	Lower/ Lower	SR	
WECC201002382	CIP-005-1	R2	Medium/ Moderate	SR	
WECC2013013087	CIP-005-3	R3; R3.2	Medium/ Severe	CA	
WECC201002269	CIP-006-1	R1; R1.6	Medium/ Severe	SR	
WECC200901632	CIP-006-1	R1; R1.8	Lower/ Lower	SR	
WECC201002273	CIP-006-1	R4	Lower/ Moderate	SR	
WECC2015014618	CIP-006-3c	R5	Medium/ Severe	SR	
WECC200801176	CIP-007-1	R1	Medium/ Severe	SR	
WECC201002260	CIP-007-1	R1; R1.1	Medium/ Severe	SR	
WECC2015014628	CIP-007-1	R2	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
WECC200902261	CIP-007-1	R3; R3.1	Lower/ Severe	SR	No Penalty
WECC2015014629	CIP-007-1	R5	Medium/ Severe	SR	
WECC201002412	CIP-007-1	R5; R5.2.2	Lower/ Severe	SR	
WECC201002279	CIP-007-1	R6; R6.4; R6.5	Medium/ Severe	SR	

WECC201002262 CIP-002-1 R1; R1.2; R1.2.2; R1.2.4 - OVERVIEW

WECC determined that URE did not consider transmission facilities at certain facilities in its Risk-Based Assessment Methodology (RBAM), in violation of CIP-002 R1. Specifically, WECC determined that URE failed to consider: 1) all assets that support reliable Bulk Electric System (BES) operations at two locations, in violation of CIP-002-1 R1.2; 2) transmission substation assets at two locations, in violation of CIP-002-1 R1.2.2; and 3) transmission assets identified as critical to system restoration at six locations, in violation of CIP-002-1 R1.2.4.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). This violation created the opportunity for misidentified or unidentified Critical Assets that pose risks associated with unidentified Critical Cyber Assets (CCAs). In this case, URE failed to consider all transmission substations and substations that support the reliable operation of the BPS or that are critical to system restoration in its RBAM. The risks posed by URE's noncompliance are, to some extent, lessened in that URE did document and implement an RBAM that resulted in identification of a number of Critical Assets including other substations and control centers.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004842-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete development and full documentation of its RBAM;
2. apply the RBAM to test its validity on a subset of URE-owned assets;

3. submit its RBAM to WECC for review;
4. discuss WECC feedback on URE's RBAM;
5. modify its RBAM, if necessary, as a result of feedback from WECC;
6. complete list of all assets for use in applying RBAM;
7. apply its RBAM to all assets; and
8. develop a list of Critical Assets for URE's area.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002354 CIP-002-1 R3; R3.1 - OVERVIEW

WECC determined that URE did not identify CCAs associated with Critical Assets located at multiple locations including substations and control centers.

WECC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Compromise of the unprotected devices could cause significant disruption of normal operations within URE's area, including the risk of substantial loss of load. In this case, URE failed to identify relays and the Control Center Cyber Assets, described herein, as CCAs. The scope of the violation includes CCAs at both URE's Control Centers and critical substations. Without proper identification, these CCAs were vulnerable to cyber security attacks.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004840-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document URE consolidated (field and control center) CCA identification methodology;
2. ensure CIP protections through obtaining attestations from CCA asset owners and/or enter into some type of agreement;
3. modify CCA identification methodology to reflect any RBAM changes that occurred as a result of feedback from WECC on URE's RBAM;
4. apply CCA identification methodology and develop list of CCAs for URE's control centers;

5. complete analysis of approaches to ensure identification and protection of CCAs at Critical Asset sites;
6. notify all asset owners of non-URE owned Critical Assets and request a list of associated Cyber Assets;
7. notify WECC of any non-URE Critical Asset owners that did not provided URE with its list of Cyber Assets, as requested above;
8. apply CCA identification methodology to develop list of CCAs for URE-owned field assets and for non-URE-owned Critical Assets;
9. notify owners of non-URE-owned CCAs of URE's CCA determination and of the need for delegation agreements;
10. complete delegation agreements; and
11. notify WECC of any non-URE Critical Asset owners for which URE has identified CCAs with which URE cannot reach agreement.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002355 CIP-003-1 R1; R1.1; R1.2; R1.3 - OVERVIEW

WECC determined that for one year, URE's cyber security policy failed to address over 20 CIP requirements, in violation of CIP-003-1 R1.1. WECC also determined that URE failed to make its cyber security policy available to all personnel with physical access to CCAs at one facility, in violation of R1.2. Finally, WECC determined that URE's CIP senior manager failed to annually review and approve one chapter in URE's cyber security policy, as required under R1.3.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Given that the one facility houses URE's Control Center and is a Critical Asset with CCAs identified by URE, noncompliance described herein potentially threatens the security of URE CCAs essential to URE Control Center operability. The risks, however, are somewhat diminished in that the cyber security policy did address 18 of the requirements for which URE was required to reach compliance. Further, the cyber security policy was made available to personnel with access to its intranet site and was posted at all but two facility entrances.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004694 to address the referenced violations. URE's Mitigation Plan required URE to:

1. ensure its CIP senior manager reviewed, approved, and issued cyber security policies on specific CIP Standards;
2. ensure its CIP senior manager reviewed and approved the grid operations information system security program manual (ISSP Manual);
3. develop a process for issuing and tracking hard copy versions of the ISSP Manual;
4. place hard-copy versions of the ISSP Manual at various points in the control centers; and
5. create awareness posters indicating location of the ISSP Manual, and send e-mail to all personnel with physical access to the control centers.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002356 CIP-003-2 R4.3 - OVERVIEW

WECC determined that although URE conducted an "annual review" of its CCA information protection program (IP Program) pursuant to CIP-003-2 R4, URE failed to assess adherence to its IP Program following implementation, in violation of CIP-003-2 R4.3

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to protect information associated with CCAs may render Cyber Assets vulnerable to misuse or malicious attack. The risks posed by URE's noncompliance are, to some extent, lessened in that URE demonstrated that it documented and implemented an IP Program.

WECC determined the duration of the violation to be from the date URE was required to assess adherence to its program, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT093456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review its ISSP Manual to ensure compliance;
2. review and revise its ISSP Manual to include process to inventory all documents requiring CIP protections;
3. complete an annual review of document inventory;
4. develop a project plan for increased scope of the potential violation;

5. complete its project plan for this Mitigation Plan;
6. develop and prepare appropriate material for identifying and protecting information that requires protection;
7. develop an information protection assessment program;
8. revise, rename, and republish ISSP Manual and related supporting documents;
9. provide CIP subject matter expert (SME) training on procedures and requirements;
10. distribute attestations and instructions to managers responsible for reviewing their organizations' CCA information;
11. provide annual entity-wide training on URE's IP Program; and
12. complete the annual assessment of adherence to the IP Program for CCA information and prepare a written report on the results of the annual assessment.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2013011670 CIP-003-3 R5 - OVERVIEW

WECC determined that URE placed two documents on its SharePoint site without implementing access management controls. Any individual with access to the SharePoint site would have had access to the documents irrespective of any authorization. WECC also determined that URE disclosed one of the documents to an external vendor that did not have authorization to view protected CCA information. Finally, URE posted videos on social media containing footage that included CCAs or facility information.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The unprotected information disclosed by URE was associated with CCAs associated with URE control centers. URE afforded these devices a number of protections. URE physically secured the devices in scope of the violation from unauthorized access within Physical Security Perimeters (PSPs). Physical access to the devices was restricted to individuals who completed personnel risk assessments (PRAs) and cyber security training. URE onsite security personnel logged and monitored physical access and physical access attempts—unauthorized access attempts would have triggered alarming.

URE also electronically secured the CCAs within an Electronic Security Perimeter (ESP). Again, individuals with electronic access to the devices completed PRAs and cyber security training. Electronic

access was restricted to individuals who required such access. Electronic access and electronic access attempts were logged and monitored. Cyber security events would have triggered alarming.

WECC determined the duration of the violation to be from the date URE posted on social media, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT008826 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise and redistribute the memorandum that designated personnel responsible for authorizing logical or physical access to protected information (as required by CIP-003-3 R5.1). This would ensure that (a) the list of personnel responsible for authorizing logical or physical access is current and (b) that the memorandum references the marking, safeguarding, and sharing of documents that contain CCA-protected information;
2. provide additional training for personnel responsible for authorizing logical or physical access to CCA-protected information and their managers regarding their responsibilities;
3. establish procedures that ensure that personnel do not allow videos and/or pictures to be taken of Control Center facilities without proper authorization; and
4. establish an agreed-upon procedure between URE's information security group and public affairs group concerning the sharing and posting of any document, video, or images that contain NERC CIP Critical Information.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801173 CIP-004-1 R2 - OVERVIEW

WECC determined that URE did not ensure it trained all personnel having access to CCAs in a special program for personnel with access to CCAs by the compliance date.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's personnel have participated in the annual cyber security and security refresher training. The relevant workstations with access to the Control Center network (CCN) are located within secure URE facilities. Cyber access and unescorted physical access to cyber assets that enable control of transmission or electric power generation is limited to personnel whose jobs require that they have access to the assets and who have completed the training required under CIP-004-1 R2.2. The CCN was a closed network. The firewall rules are defined based on the policy that no connections initiated external to the ESP of the CCN are permitted inbound through the ESP firewall.

Network intrusion detection devices are installed on all network segments internal and external to the ESP of the CCN. Personnel with administrative cyber access rights to CCAs are identified, and access is limited to maintenance personnel. Access to control center CCAs is limited to entity employees and contractor employees. Physical access is controlled through combinations of identification cards, proximity card key access control systems, closed circuit cameras, and/or security personnel. CCAs are monitored continuously by control center maintenance personnel to ensure they are functioning properly.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-08-1205 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training on control center CCAs;
2. identify changes to the ESP, PSP, and CCA security controls to further limit access to CCAs;
3. implement changes identified above;
4. identify and train any remaining personnel with cyber and unescorted physical access to control center CCAs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801174 CIP-004-1 R3 - OVERVIEW

WECC determined that URE did not complete PRAs for all contractor employees by the compliance deadline.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All URE employees have had the required background investigation, although not all have been reassessed in the last seven years. URE's process has required identity verification of all new URE and contract employees for over ten years. Therefore, the risk of current URE or contract employees never having had a background investigation is low.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT081206 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014185 CIP-004-3a R3 - OVERVIEW

WECC determined that URE did not update one PRA that expired after seven years for a contract employee in good standing.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented preventative controls, such as multiple layers of user names and passwords with varying levels of clearance, which the person in scope did not have, to get access to CCAs. URE also uses two-factor authentication, requiring a randomly generated number in addition to a four-digit PIN, neither of which the person in scope had. URE implemented detective controls, such as logs of all physical access attempts, both successful and unsuccessful, which would allow the entity to know if/when the person in scope entered a substation. URE monitors all trip and close operations, which generate alarms to alert personnel of issues. Personnel also receive alarms for unauthorized breaker operations or relay failures. As a corrective control, URE personnel can remotely operate relays and breakers to maintain system stability. URE also has procedures to respond to emergencies. As compensating controls, URE logically separates its substations, not allowing anyone with access to one substation to access other substations, meaning that a malicious person would have to go to each substation to load a virus, which could give the entity more time to detect any issues.

WECC determined the duration of the violation to be from the date URE should have updated the PRA, through when URE completed the PRA.

URE submitted its Mitigation Plan designated WECCMIT010933 to address the referenced violations. URE's Mitigation Plan required URE to:

1. make minor revisions of the PRA verification checklist to include a reviewer verification field; and
2. make modifications to the standard operating procedure (SOP) to include verbiage that instructs staff not to approve initial PRA verification requests when the PRA is within six months of expiration. Instead the staff member whose PRA is expiring will be contacted and notified that they must complete the PRA renewal process before approval is granted.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002280 CIP-004-1 R3; R3.2 - OVERVIEW

WECC determined that URE did not update each PRA at least every seven years after the initial PRA. In a second instance, WECC determined that URE failed to conduct a PRA within 30 days of personnel receiving access to CCAs. Finally, URE identified three additional instances wherein it granted access to CCAs to personnel without completing a recurring PRA every seven years.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All employees did complete and pass initial identity verification. Further, all employees underwent a criminal background check at the time of hiring.

WECC determined the duration of the violation to be from 30 days after URE granted access to an employee without the employee having a valid PRA, through when URE completed all recurring PRAs.

URE submitted its Mitigation Plan designated MIT-09-3456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop e-mail templates to notify organizations which grant or revoke authorized unescorted physical or cyber access;
2. complete a review of hard-copy documentation for all employees having authorized cyber or authorized unescorted physical access to CCAs;
3. document procedures for a quarterly random sample review of hard-copy documentation of seven-year criminal check and personal identity verification;
4. revoke cyber and/or physical access to CCAs for employees without a timely criminal check and personal identity verification;
5. complete seven-year criminal checks and personally identify verification for any employees whose access was revoked above;

6. review all SOPs regarding criminal checks and personal identity verifications to ensure they provide adequate quality assurance and quality control measures.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801175 CIP-004-1 R4 - OVERVIEW

WECC determined that URE did not fully document the specific electronic or unescorted physical access rights of all URE personnel with access to CCAs by the compliance date. The ESP of the Control Center network (CCN) expanded beyond the PSP of the Control Center.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All workstations with CCN access are located within secure URE facilities. URE requires all employees complete mandatory Annual Cyber Security and Security Refresher Training on URE policies pertaining to the protection of all URE sensitive information and information systems including CCAs. Cyber access and unescorted physical access to critical cyber assets that enable control of transmission or electric power generation is limited to Control Center users and support staff. The CCN is a closed network. The firewall rules are defined based on the policy that no connections initiated external to the ESP of the CCN are permitted inbound through the ESP firewall. Network intrusion detection devices are installed on all network segments internal and external to the ESP of the CCN. Personnel with administrative cyber access rights to CCAs are identified. Access to Control Center CCAs is limited to URE employees and contract employees. Physical access is controlled through identification cards, proximity card key access control systems, closed circuit cameras, and security personnel. Control center maintenance personnel continuously monitor the proper functioning of CCAs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-08-1207 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training on control center CCAs;
2. identify changes to the ESP, PSP, and CCA security controls to further limit access to CCAs;
3. implement changes identified above; and
4. identify and train any remaining personnel with cyber and unescorted physical access to control center CCAs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002381 CIP-005-1 R1 - OVERVIEW

WECC determined that URE did not identify three Control Center ESP (CORE ESP) access points. WECC determined that URE implemented a "rule change that allowed external access" resulting in the firewalls no longer being isolated within the CORE ESP. Rather, the firewalls became access points to the CORE ESP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not identify the three firewalls as "ESP access points," URE implemented electronic access controls and monitoring at each firewall by virtue of an internal policy requiring firewalls to be protected in a manner consistent with CIP-005 R2. URE's layered security required further authentication before accessing other Cyber Assets within the ESP.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004842 to address the referenced violations. URE's Mitigation Plan required URE to:

1. validate all current network access points to the ESP, review the current ESP, and check related documentation including access point and network diagrams;
2. update the Control Center ESP plan to reflect new configuration and publish the updated ESP; and
3. update any additional procedures and operational documentation required, including access point administration.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201102851 CIP-005-1 R1; R1.4 - OVERVIEW

WECC determined that URE did not identify at least 15 devices as Cyber Assets within an ESP. The devices were associated with two Critical Assets.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Risk was limited by compensating measures in place during the violation period.

All Cyber Assets were located within a PSP. Although URE did not identify the devices as Cyber Assets, it did afford some logical protection because all of the devices were also located within the ESP. URE's layered security network further limited electronic access to the devices.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004842 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review process(es) for determining whether electronic assets within the Control Center ESP are Cyber Assets;
2. develop and publish the policy and process for determining whether electronic assets are Cyber Assets;
3. review, update, publish, and implement the process and procedures to introduce and protect new Cyber Assets within a defined ESP based upon the policy developed above;
4. update its list of devices and determine/document which devices on the updated list are Cyber Assets within the Control Center ESP; and
5. submit any required Technical Feasibility Exceptions (TFEs).

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200901633 CIP-005-1 R1; R1.5 - OVERVIEW

WECC determined that URE did not have a documented PRA program for personnel associated with Cyber Assets used in the access control and monitoring of the ESP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had previously performed background screening for its personnel. This violation occurred only because URE did not update these background checks and perform PRAs, as it had not yet completed developing its CIP-004-1 R3 PRA program.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-2002 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002382 CIP-005-1 R2 - OVERVIEW

WECC determined that URE did not document the organizational processes and technical and procedural mechanisms for control of electronic access points at three CORE ESP access points.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although a failure to identify ESPs can render CCAs and associated Critical Assets vulnerable to compromise, a number of compensating factors unique to URE's cyber network in this case lessens the risks. Although URE did not identify the three firewalls as "ESP access points," URE implemented electronic access controls and monitoring at each firewall with an internal policy requiring that all firewalls have protections in a manner consistent with CIP-005 R2. URE's layered security required further authentication before accessing other Cyber Assets within the ESP.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT004843 to address the referenced violations. URE's Mitigation Plan required URE to:

1. validate all current network access points to the ESP, review the current ESP, and check related documentation including access point and network diagrams;
2. update the Control Center ESP plan to reflect new configuration and publish the updated ESP; and
3. update any additional procedures and operational documentation required, including access point administration.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2013013087 CIP-005-3 R3; R3.2 - OVERVIEW

WECC determined that URE did not have a security monitoring process that alerts designated response personnel to unauthorized access attempts and for actual unauthorized access. While URE logged access and access attempts, URE did not provide alerts to appropriate personnel to respond in the event of unauthorized attempts or actual access.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented several physical and logical layers of defense that would likely have prevented and/or detected unauthorized users from logging into any access point protecting CCAs and Electronic Access Control or Monitoring Systems (EACMS). First, URE implemented restricted ports and services and did not allow all traffic to pass through the access points. Second, Intrusion Detection System (IDS) sensors were placed in-line for most access points to the ESP, which would have likely detected any abnormal network traffic or abnormal conditions passing into or out of the ESP. Third, URE has well-trained personnel who monitor network traffic continuously who could have responded immediately to any cyber security attacks or other malicious traffic. Finally, access to the access points is limited to a small group of technicians who must physically be at one of the control centers in order to login and make any type of configuration changes. As such, the probability of someone attempting to login without authorization is extremely limited.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT010947-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify ESP access point events that require automated alerting, at a minimum, to include alerts for login processes;
2. use list of ESP access events to identify gaps in automated alerting and logging processes;
3. create new processes to capture, correlate, and alert on ESP access point logs events;
4. implement any new automated alerting; and
5. train staff on new process.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002269 CIP-006-1 R1; R1.6 - OVERVIEW
WECC determined that on five occasions, URE did not ensure it escorted visitors continuously within the PSP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although visitors were found without their escorts, URE security personnel on site quickly identified visitors and escorted visitors and their escorts from the building. Visitor access to and movement within the site was monitored by video and by URE personnel. Visitors did not have access to CCAs.

WECC determined the duration of the violation to be from when the first unescorted access occurred, through when access was revoked for the last instance of noncompliance.

URE submitted its Mitigation Plan designated MIT-10-3072 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop procedures related to unescorted physical access for use when control centers are staffed with contracted security personnel;
2. provide refresher training;
3. update training program for security personnel;
4. review procedures regarding physical access to and from the loading dock into and out of the building;
5. interview and retrain the personnel at issue;
6. review service contract clauses to ensure authority to take action, including termination, for failing to follow URE policies;
7. provide all contractors with training information related to continuous escort;
8. conduct e-mail outreach regarding continuous escorted access within PSPs;
9. place posters on continuous escorted access near control center entrances;
10. review escort badging process procedures and implement any new requirements;
11. revise system operations hardware maintenance organizations incident response plan to ensure all incidents are referred to URE security;
12. develop alternatives for access modifications to the areas with CCAs in the facility at issue to reduce the size of the PSP;

13. review the visitor access control program for modifications for the reduced sized PSP are warranted;
14. approve the final design(s) for access modifications to the areas with CCAs and proceed with construction;
15. implement the new PSP; and
16. revise internal documents to reflect changes to the visitor access program, implement the changes, and notify all affected employees of the changes.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200901632 CIP-006-1 R1; R1.8 - OVERVIEW

WECC determined that URE's physical security plan did not address a PRA program for personnel associated with Cyber Assets used in the access control and monitoring of the PSP.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had previously performed background screening for all its personnel. This violation occurred only because URE did not update these background checks and perform PRAs, as it had not yet completed developing its CIP-004-1 R3 PRA program.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-2001 to address the referenced violations. URE's Mitigation Plan required URE to:

1. establish a process for URE to perform recurring PRAs;
2. inform union representatives of the recurring PRAs;
3. identify all individuals required to undergo a recurring PRA;
4. develop processes and procedures for ensuring ongoing compliance; and
5. process all individuals requiring a recurring PRA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002273 CIP-006-1 R4 - OVERVIEW
WECC determined that URE did not implement technical or procedural mechanisms to generate access logs consistent with CIP-006-1 R4 at six PSP access points.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did provide card reader logs for all access points. The building at issue did contain video surveillance as well as security personnel to monitor activity within the building. Further, URE cyber security policy and training prohibited visitor and tailgater access at each of the six access points.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-3120 to address the referenced violations. URE's Mitigation Plan required URE to:

1. consult with URE security and emergency response organization to provide video detection at all of the access points into the facility to ensure that physical access is logged with sufficient information to uniquely identify individuals and to identify tailgaters;
2. select video detection alternative; and
3. complete installation and testing of new equipment.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014618 CIP-006-3c R5 - OVERVIEW
WECC determined that URE did not monitor physical access at all access points to the PSP for approximately 35 hours while its security system was without power.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. When the security system lost power, all access points locked. In order to get through the locked door, personnel were required to contact security to get a combination for a lock box that contained a key to the substation. As a compensating measure, personnel were onsite at various times throughout the outage, thereby shortening the time available for an intruder to cause harm.

WECC determined the duration of the violation to be from when URE failed to continuously monitor access to the PSP, through when URE began continuously monitoring access to the PSP.

URE submitted its Mitigation Plan designated WECCMIT011444-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review and update the physical security response plan with all stakeholders, including identification of stakeholder roles and responsibilities;
2. create detailed procedures, or modify existing procedures, that will align with or support the response plan as required;
3. obtain stakeholder approval for final version of URE response plan;
4. develop change management process to implement for training and awareness on requirements outlined within physical security response plan and stakeholder response plans;
5. execute and complete change management process; and
6. implement physical security response plan and the stakeholder response plans.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200801176 CIP-007-1 R1 - OVERVIEW

WECC determined that URE has manual test procedures to test existing security controls. However, due to size and scope of the relevant URE assets, URE failed to determine if any changes affected the security controls of those assets

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintains parallel environments for Critical Cyber Systems with fail-over protection, minimizing the impact of a failure.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-08-1208 to address the referenced violations. URE's Mitigation Plan required URE to:

1. commission a new tool for security testing;
2. validate proper functioning of the tool;
3. complete automated tests of those assets to form a baseline of existing security controls; and
4. develop procedures to use the new automated tool to test the compliance of systems.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002260 CIP-007-1 R1; R1.1 - OVERVIEW

WECC determined that URE did not create a testing program pursuant to CIP-007 R1 for indicated Cyber Assets and systems; URE failed to test "significant changes" prior to implementation; and URE failed to document any test results. URE failed to create, implement, and maintain a procedure for cyber security testing and failed to examine "rule change" effects on cyber security controls.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Risks posed by noncompliance were, to some extent, reduced given a number of compensating measures in place during the violation period. URE implemented network-scanning tools on segments throughout the ESP in scope. In addition, the ESP has extensive IDS. URE stated that access to an account on its host does not provide access to any relevant domains or hosts, including CCA hosts.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-08-3474-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify existing technical security controls that could be adversely affected by the addition of a new Cyber Asset or a significant change to an existing Cyber Asset;
2. for controls identified above, identify whether adequate test procedures exist, need to be developed, or existing procedures need to be updated;
3. provide status on development or update of test procedures identified above;
4. complete the development or update of test procedures identified above;
5. train staff on new or updated test procedures;
6. review and update internal documents to require testing of cyber security controls for URE-developed executable code and testing of cyber security controls for third-party software or firmware for new Cyber Assets and for significant changes to existing Cyber Assets within the ESP;

7. review and update existing application-specific test plans to require testing of cyber security controls for URE-developed executable code for new Cyber Assets and for significant changes to existing Cyber Assets within the ESP;
8. review and update the transmission services procedures;
9. provide training for appropriate staff;
10. publish and implement all updated documents; and
11. prepare written report on implementation results.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014628 CIP-007-1 R2 - OVERVIEW

WECC determined that URE did not establish and document a baseline of the ports and services required for normal or emergency operations and ensure that it enabled only those ports and services for 27 devices.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE configured the access points in front of the devices in scope to allow only certain traffic to get to the devices. Even if a port and service were open on a device, the access point might not allow traffic on that port. The access point also is set up to deny all traffic not explicitly allowed in the Access Control List (ACL). URE also uses up-to-date anti-malware that prevents and detects malware attacks designed to compromise the devices. Finally, URE also implemented strong detective controls to detect access to the devices. Specifically, URE uses a security status monitoring utility which could have detected an attempt to compromise the devices.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011457 to address the referenced violations. URE's Mitigation Plan required URE to:

1. verify that only needed ports and services are enabled, as technically feasible, on the devices in scope of the violation; and
2. update the ports and services documentation for the devices in scope of the violation.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200902261 CIP-007-1 R3; R3.1 - OVERVIEW
WECC determined that URE did not assess or implement 13 patches for three Cyber Assets within 30 days of availability.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE implemented network scanning tools that covered the Cyber Assets in scope. Additionally, the ESP containing Cyber Assets has extensive intrusion detection and protection systems in place. Further, the system host does not provide access to domains or hosts, including CCA operating system hosts.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-3283 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete the assessment of security patches and security upgrades for the open training systems. Document compensating measures to mitigate risk exposure or document acceptance of risk for any patches or upgrades that will not be installed, if any;
2. review remaining software inventory to determine whether security patches or security upgrades were neither installed nor assessed;
3. complete and document the assessment of security patches and security upgrades;
4. for any security patches not installed, either document compensating measures to mitigate risk exposure or document acceptance of risk;
5. review and update security patch process documents as necessary; and
6. provide refresher training on the security patch process.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014629 CIP-007-1 R5 - OVERVIEW
WECC determined that URE did not establish, document, and implement a policy to minimize and manage the scope and acceptable use of factory default accounts for 27 devices.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE had strong preventative controls to prevent unauthorized access. URE implemented a software patch program to ensure that all applicable security-related software patches were installed or, if not installed, had compensating measures to mitigate risk. URE also uses an anti-virus program, which could prevent an attempted malware attack. Additionally, URE implemented a program to enable those ports and services necessary for operation on the access points to the ESP, denying access by default. If a malicious person discovered a vulnerable port and service, malware targeted to only that port would need to pass through the access point, which could stop the attack. In addition, URE implemented strong detective controls to detect unauthorized access. Specifically, URE uses a security testing system that constantly monitors the open ports and services on a device. If a port or service is enabled that is not on the baseline, personnel are alerted, which could allow them to detect a malicious person who is trying to compromise devices on the network. URE is also logging security events on the above devices, which could alert URE to a possible malware attack.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011456 to address the referenced violations. URE's Mitigation Plan required URE to:

1. examine the default accounts and remove, disable, or rename them where possible. If the account must remain enabled, URE would:
    a. identify individuals who have authorized access to the account;
    b. change the default password per Cyber Asset capability;
    c. enforce minimum password complexity requirements either technically or procedurally; and
    d. enforce password changes at least annually where technically or procedurally feasible.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

<u>WECC201002412 CIP-007-1 R5; R5.2.2 - OVERVIEW</u>
WECC determined that URE did not identify one user with access to a shared account on the Control Center server (a supervisory control and data acquisition (SCADA) server) and failed to change passwords annually for two shared accounts on a second Control Center server.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had security measures in place during the violation period, including access monitoring, logging, and alarming, as well as URE's cyber security training program for all URE employees.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-3531 to address the referenced violations. URE's Mitigation Plan required URE to:

1. review all individual and shared accounts subject to CIP-007 R5;
2. disable the account or identify the individuals with access for all shared accounts for which users with access are not identified;
3. disable the account or change the password for all accounts that have a password older than 13 months;
4. review account management plans for all Cyber Assets subject to CIP-007 R5 and identify which revisions and/or additions to existing annual password change technical and/or procedural controls are necessary;
5. review existing annual user account procedures and identify which, if any, procedures need to be revised to ensure that all individual and shared accounts are addressed;
6. update account management plans to document revisions and/or additions to annual password technical and/or procedural controls, as necessary;
7. update annual user account review procedures, as necessary; and
8. train appropriate staff on revisions and additions to security controls and procedures.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002279 CIP-007-1 R6; R6.4; R6.5 - OVERVIEW

WECC determined that URE did not retain logs of system events related to cyber security for 90 days for a single Cyber Asset, in violation of R6.4. WECC also determined that URE failed to review logs prior to removal, in violation of R6.5.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Access to the Cyber Asset is limited. In addition, the ESP containing the Cyber Asset has no remote access and requires users first to physically access the Control Center PSP before logging into the network. Further, although URE did not maintain logging, the firewall was equipped with alarming which would trigger in the event of logical unauthorized access attempts.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated MIT-09-3284 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document decision to replace management console and firewall appliance;
2. follow established procedures for installing a checkpoint firewall;
3. decommission the management console and the firewall appliance following standard procedures;
4. follow established log management procedures for checkpoint firewalls; and
5. document that logs have been retained for 90 calendar days using the new firewall and perform required review.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has not assessed a penalty for the referenced violation. In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;

2. URE had an internal compliance program (ICP) at the time of the violations which WECC considered a mitigating factor;

3. URE has invested significant time and effort to implement its ICP. WECC considers URE's use of a rapid response team for the self-reporting process to be an exemplary practice. This rapid response team has specific time-based performance targets.

4. URE self-reported the majority of the violations;

5. URE was cooperative throughout the compliance enforcement process;

6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. at no time did any disturbance or outage, or actual harm to the BPS, result from these violations

8. the violation of CIP-002-1 R3 posed a serious or substantial risk to the reliability of the BPS, as discussed above; and

9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, no penalty is appropriate.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC

BOTCC reviewed the Settlement Agreement and supporting documentation on December 16, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 28, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1, Unidentified Registered Entity 2, Unidentified Registered Entity 3, and Unidentified Registered Entity 4, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), Unidentified Registered Entity 2 (URE2), Unidentified Registered Entity 3, and Unidentified Registered Entity 4 (Collectively the URE Entities), with information and details regarding the nature and resolution of the violations,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE Entities have entered into a Settlement Agreement to resolve all outstanding

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2015). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

issues arising from ReliabilityFirst's determination and findings of violations of the CIP Reliability Standards.

According to the Settlement Agreement, URE Entities neither admit nor deny the violations, and have agreed to the assessed penalty of one hundred and fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Accordingly, NERC is filing this Full Notice of Penalty in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between ReliabilityFirst and URE Entities. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013798	CIP-002-3	R3	High/ Severe	SC	$150,000
URE1 RFC2014013829	CIP-003-3	R1	Medium/ Severe	SR	
URE1 RFC2014013830	CIP-003-3	R4	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013799	CIP-003-3	R5	Lower/ Severe	SC	
URE1 RFC2014013800	CIP-003-3	R6	Lower/ Severe	SC	
URE1 RFC2014013831	CIP-004-3	R1	Lower/ Severe	SR	
URE1 RFC2014013832	CIP-004-3	R2	Lower/ Severe	SR	
URE2 RFC2014013446	CIP-004-3a	R2.1	Medium/ Severe	SR	
URE1 RFC2014013801	CIP-004-3	R4	Lower/ Severe	SC	
URE2 RFC2014013794	CIP-004-3a	R4.1	Lower/ Severe	SC	
URE1 RFC2014013802	CIP-005-3a	R1	Medium/ Severe	SC	$150,000
URE1 RFC2014013803	CIP-005-3a	R2	Medium/ Severe	SC	
URE1 RFC2014013804	CIP-005-3a	R3	Medium/ Severe	SC	
URE1 RFC2014013805	CIP-005-3a	R4	Medium/ Severe	SC	
URE1 RFC2014013833	CIP-005-3a	R5	Lower/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013810	CIP-006-3c	R1	Medium/ Severe	SC	
URE2 RFC2015014715	CIP-006-3c	R1	Medium/ Severe	SR	
URE1 RFC2014013811	CIP-006-3c	R2	Medium/ Severe	SC	
URE1 RFC2014013812	CIP-006-3c	R3	Medium/ Severe	SC	
URE4 RFC2014013809	CIP-006-3c	R3	Medium/ Severe	SC	
URE1 RFC2014013813	CIP-006-3c	R4	Medium/ Severe	SC	
URE1 RFC2014013814	CIP-006-3c	R5	Medium/ Severe	SC	
URE1 RFC2014013815	CIP-006-3c	R6	Lower/ Severe	SC	$150,000
URE1 RFC2014013834	CIP-006-3c	R7	Lower/ Severe	SR	
URE1 RFC2014013835	CIP-006-3c	R8	Medium/ Severe	SR	
URE1 RFC2014013820	CIP-007-3a	R1	Medium/ Severe	SC	
URE1 RFC2014013821	CIP-007-3a	R2	Medium/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2015015243	CIP-007-3a	R3	Lower/ Severe	SR	$150,000
URE2 RFC2014013795	CIP-007-3a	R3	Lower/ Severe	SC	
URE1 RFC2014013822	CIP-007-3a	R4	Medium/ Severe	SC	
URE1 RFC2014013823	CIP-007-3a	R5	Lower/ Severe	SC	
URE2 RFC2014014469	CIP-007-3a	R5.2.3	Lower/ Severe	CA	
URE3 RFC2014013797	CIP-007-3a	R5	Lower/ Severe	SC	
URE4 RFC2014013816	CIP-007-3a	R5	Lower/ Severe	SC	
URE1 RFC2014013824	CIP-007-3a	R6	Lower/ Severe	SC	
URE1 RFC2014013915	CIP-007-3a	R7	Lower/ Severe	SR	
URE1 RFC2014013825	CIP-007-3a	R8	Lower/ Severe	SC	
URE1 RFC2014013836	CIP-007-3a	R9	Lower/ Severe	SR	
URE1 RFC2014013826	CIP-008-3	R1	Lower/ Severe	SC	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Penalty Amount
URE1 RFC2014013827	CIP-009-3	R1	Medium/ Severe	SC	

Background

ReliabilityFirst resolved all of these violations together because the URE Entities all share a common parent company and now implement the parent company's unified CIP compliance program.

Prior, the current parent company acquired URE1 from its original parent company and acquired another subsidiary company that controlled some of the operations of the original parent company. After a number of events, the original parent company filed for Chapter 11 bankruptcy. The bankruptcy filing caused uncertainty regarding the future of the original parent company and its subsidiary company, thus resulting in voluntary departures from both organizations. The loss of resources and leadership in personnel actively engaged in the CIP compliance program created a foundation for the violations.

Before the acquisition of URE1, the current parent company merged with the former parent company of URE2, URE3, and URE4. Although URE2, URE3, and URE4 continue to operate under the former parent company umbrella, the current parent company became the legal owner of that umbrella company and is now the ultimate parent company for the three URE Entities included in this Settlement Agreement.

After these acquisitions, the current parent company updated its CIP compliance program so that the parent and its subsidiaries have one unified CIP compliance program.

RFC2014013798 CIP-002-3 R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary company violated CIP-002-3 R3 by failing to identify, as part of its Critical Cyber Asset identification process, multiple devices as Critical Cyber Assets (CCAs) that were essential to the operation of its Critical Assets. Specifically, the former subsidiary company failed to appropriately classify as CCAs several devices that used a routable protocol to communicate outside of the Electronic Security Perimeter (ESP) or used a routable protocol to communicate within a control center.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). First, an accurate list of CCAs is fundamental to ensuring that all CCAs are afforded the protections required by the CIP Reliability Standards. Therefore, former subsidiary's failure to maintain an accurate list of CCAs increases the likelihood of further violations of other CIP Reliability Standards. Second, the duration of the violation indicates that the subsidiary failed to identify and correct the issue in a timely manner, which also increased the likelihood of further violations of other CIP Reliability Standards. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary had several measures in place to protect and restrict access to the mistakenly excluded CCAs both logically and physically. Logically, these devices were protected by being on a restricted network, having password protections on the connections to the network systems, and several other protective measures including intrusion detection, logging, and anti-malware programs. Physically, access to these devices was also highly restricted to authorized personnel with multiple physical access control layers within a non-public, controlled space. These devices were in a secured facility and under constant surveillance.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011314 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. use the current parent company's CCA identification program to ensure that processes are in place to include consideration and identification of all Cyber Assets;
2. identify all applicable Cyber Assets;
3. implement the current parent company's CCA Identification Program to ensure that all CCAs are identified and documented; and
4. provide training for all appropriate personnel regarding CCA identification.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013829 CIP-003-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary company violated CIP-003-3 R1 by failing to document and implement a cyber security policy that addressed all of the aspects required by CIP-003-3 R1. Specifically, the deficient cyber security policy: a) did not adequately address the requirements of CIP-002-3 through CIP-009-3; and b) was annually reviewed, but was not reviewed and approved by the senior manager assigned pursuant to R2.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary did have a documented and implemented cyber security policy that represented management's commitment and ability to secure its CCAs. This policy was annually reviewed by the subsidiary's management, but not by the senior manager identified in CIP-003-3 R2.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when the subsidiary formally adopted and implemented an adequate cyber security policy.

URE1 submitted its Mitigation Plan designated RFCMIT011234 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. modify the cyber security policy and the security management controls program documentation to include the necessary elements for compliance with CIP-003-3; and
2. approve the cyber security policy and the security management controls program.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013830 CIP-003-3 R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R4 by failing to implement and document a program to identify, classify, and protect information associated with CCAs as required by CIP-003-3 R4. Furthermore, even after formalizing the security management controls program, the subsidiary had not yet annually assessed adherence to its CCA information protection program, including documentation of the assessment results as required by CIP-003-3 R4.3.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal, documented security management controls program prevents an entity from ensuring that responsible personnel are performing the necessary activities to protect CCA information. An undocumented program increases the likelihood of human error, which may result in protected CCA information being compromised. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. First, the generation assets potentially affected by this violation have not been determined to be critical. Second, the logical and physical access controls in place with respect to CCAs also operate to protect CCA information.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011225 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the security management controls program that identifies, classifies, and protects information associated with CCAs as required by CIP-003-3 R4 and 4.1;
2. develop and document an assessment methodology to assess the adherence to the CCA information protection program;
3. assess the adherence to the CCA information protection program, including documentation of the assessment results as required by CIP-003-3 R4.3;
4. implement an action plan to remediate deficiencies identified during the assessment; and
5. train individuals responsible for the protection of CCA information and assessment of the program to ensure ongoing compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013799 CIP-003-3 R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R5 by failing to: a) have a documented program for managing access to protected CCA information; b) annually verify the list of personnel responsible for authorizing access privileges to protected information to confirm that access privileges were correct and that they corresponded with the subsidiary's needs and appropriate personnel roles and responsibilities; and c) assess and document the processes for controlling access privileges to protected information.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The access controls called for by CIP-003-3 R5, specifically maintaining an access list and performing periodic verification of logical and physical access to protected information, are an integral part of an entity's CIP compliance program. Thus, inadequate access controls may allow for unauthorized access to such information and may result in violations of several other CIP Reliability Standards and Requirements. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. First, the logical and physical access controls in place with respect to CCAs also operate to protect CCA information. Second, the subsidiary stored relevant information

on restricted networks and limited access to those individuals with a business need to access the information.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011221 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation which details program for managing access to protected CCA information as required by CIP-003-3 R5 and 5.1;
2. verify and create the list of personnel responsible for authorizing access to protection information;
3. have approved individuals review the list of user access privileges and roles and responsibilities to ensure that the list is appropriate;
4. develop and document an assessment methodology to assess the process for controlling access privileges to protected information;
5. assess the process for controlling access privileges to protected information, including documentation of the assessment results; and
6. train individuals, who are responsible for the program for managing access to protected CCA information, on the process to ensure ongoing compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013800 CIP-003-3 R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-003-3 R6 by failing to have a formally documented change control or configuration management process for the activities required in R6. Rather, the subsidiary only had an informal change management process including a ticketing system to approve and track master change requests for all changes to CCAs as well as other Information Technology (IT) assets.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of a formal change control and configuration management process can result in serious vulnerabilities and increased threat levels. Without such a process, an entity may be unable to identify unauthorized changes to its system or to determine the extent of a possible intrusion. The

risk posed by the foregoing facts and circumstances was mitigated by subsidiary's informal change management process that was in place during the period of noncompliance. As stated above, this informal process included a ticketing system to approve and track master change requests for all changes to CCAs as well as other IT assets.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011215 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop a formal, documented change management processes for compliance with CIP-003-3; and
2. approve the documented change management processes to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013831 CIP-004-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R1 by failing to document its security awareness program to ensure that personnel with authorized cyber or unescorted physical access to CCAs received ongoing awareness reinforcement in sound security practices. Rather, the subsidiary only had an informal, undocumented communication plan in place for security awareness for such personnel.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal security awareness program increases the likelihood that responsible personnel may not be aware of the latest security threats. Cyber threats, in particular, are constantly evolving, which requires responsible personnel to keep updated on an ongoing basis. The risk posed by the foregoing facts and circumstances was mitigated by the informal communication plan that the subsidiary had in place. Pursuant to this plan, responsible personnel would keep each other updated on any new threats or security issues of which they became aware.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011216 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security awareness and training program for CIP-004-3a; and
2. approve that documentation.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013832 CIP-004-3 R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R2 by failing to have a documented cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCAs. Moreover, once the subsidiary implemented a program, the training did not specifically address the minimum topics included in the sub-requirements of CIP-004-3 R2. Specifically, the program did not cover action plans and procedures to recover or re-establish CCAs and access thereto following a cyber security incident. Additionally, while this recovery training was provided as ancillary training, not all relevant personnel were involved.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of a formal cyber security training program increases the likelihood that untrained personnel may have cyber or unescorted physical access to CCAs. In this case, at least some of the subsidiary's personnel, who were responsible for recovery following a cyber security incident, were not involved in any training related to recovery testing.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011226 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal, documented annual cyber security training program, and train all responsible individuals on the annual cyber security training program to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013446 CIP-004-3a R2.1- OVERVIEW

ReliabilityFirst determined that on two separate occasions, both of which occurred prior to URE2's transitioning to the current parent company's CIP compliance program, URE2 granted certain individuals, who had not completed the requisite training, access to a Physical Security Perimeter

(PSP). A security officer, who was newly hired by a contracted security service, erroneously escorted a cleaning crew into a designated PSP without proper authorization and documentation. The cleaning crew remained within the PSP for a total of 25 minutes. On a different occasion, an individual was granted access to a PSP without proper training during the commissioning of a new PSP area. Although URE2 had completed a Personnel Risk Assessment (PRA) for this individual, he had not completed the required training prior to obtaining access. URE2 removed his access on a later date that year.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In the first instance, the cleaning crew was escorted into the PSP by an individual with authorized unescorted physical access. The cleaning crew was in the PSP for only a short period of time during which CIP-trained and authorized personnel were present and observed the cleaning crew's actions. In the second instance, the individual had passed the PRA. ReliabilityFirst also notes that access records indicate that this individual did not access the PSP during the time he had unauthorized access to it.

ReliabilityFirst determined the duration of the violation to be from the date that the cleaning crew was improperly granted access to a PSP in the first instance, through the date on which URE2 removed PSP access for the individual in the second instance.

URE2 submitted its Mitigation Plan designated RFCMIT011423-1 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. change the security officers' passwords to prevent sharing;
2. ensure that hard copies of security procedures are readily available at the security desk;
3. assign unique credentials to each security officer to further prevent sharing among security officers;
4. review current practices and guidelines for providing NERC CIP physical access and visitor access, lost or forgotten identifications and/or passwords, and escort requirements; and
5. develop a process of notification when security officers are requested to be added, changed or removed, a change ticket must be completed to ensure that new officers received proper training, background checks, and are receiving the appropriate access or revocation.

RFC2014013801 CIP-004-3 R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-004-3 R4 by failing to maintain complete lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs, missing 15% or more of the

authorized personnel. Furthermore, the subsidiary did not review the list(s) of all personnel who have access to CCAs quarterly, nor did the subsidiary update the list(s) within seven calendar days of any change of personnel with such access to CCAs, nor any change in the access rights of such personnel. The subsidiary also failed to revoke access to CCAs within 24 hours for personnel terminated for cause nor within seven calendar days for personnel who no longer required such access to CCAs.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The failure to maintain a current and accurate list of personnel with cyber or unescorted physical access to CCAs increases the likelihood that a cyber-attacker could obtain unauthorized access to the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by several additional controls that were in place during the period of noncompliance. For instance, access to the CCAs was highly restricted both physically and logically. All currently identified CCAs are in a secured facility with multilayered physical security controls to restrict physical access. The primary assets are located in a secured data center which provides an attestation of the controls environment and the backup generation management system (GMS) is located in a secured room. The CCAs are also continuously monitored and logged, sit behind an ESP with intrusion detection, have antivirus and malware prevention tools installed, and are contained within a restrictive network.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011235 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's access control program to install the Energy Management System (EMS) integrated system on the affected CCAs to ensure that the proper processes are in place for quarterly review and update of the Master Access List;
2. identify individuals who should be on the Master Access List prior to the EMS migration;
3. review and certifying that each individual to be authorized has completed the appropriate credentials and document the authorization updates within the Master Access List; and
4. train appropriate personnel on the actions necessary for compliance with CIP-004-3 R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013794 CIP-004-3a R4.1- OVERVIEW

ReliabilityFirst determined that prior to transitioning to the current parent company's CIP compliance program, URE2 violated CIP-004-3a R4 by: a) failing to update its CCA personnel access list within 7 days of an access change; and b) granting PSP access to an individual who did not receive access approval for that area.

For the first instance, during the integration of URE2, URE3, and URE4 and the current parent company and the corresponding installation of the EMS system, access change requests were submitted via multiple ticketing systems. The parties responsible for maintaining the access documentation were not receiving all of the necessary notifications of access requests. Consequently, those responsible individuals failed to update the access lists within the appropriate time frame. In all cases, the access was approved and proper PRAs were performed.

For the second instance, during the commissioning of a new PSP, an individual was granted access to the new PSP without proper approval. Prior to the declaration of the area as a PSP, but after construction was completed, access was provided to those individuals working in the new room. Due to the number of individuals with access to the area, the normal ticketing process was not used where a ticket for each individual would have been entered. Instead, all parties requiring access were processed as a group with PRA and training being tracked prior to requesting approval for access. Although the individual was on the original group tracking list, he was not on the list submitted for approval. On the date the individual needed access, the individual required access to the area for the first time. The access provider, seeing his name on the original tracking list, assumed he was approved for access and provided an access card. Since the individual was not included in the original group approval, he did not have proper approval for access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although access changes were not completed within the appropriate timeframe, all access changes were approved and PRAs were completed. In addition, logical access controls were still in place. Specifically, the devices at issue are enclosed within an ESP protected by firewalls and monitored per the CIP-005-3 requirements. Moreover, the devices at issue were located on isolated networks to prevent exposure to untrusted networks. Second, the instances of noncompliance were the result of unique circumstances which occurred during the merger between URE2 and the current parent company, but prior to URE2's transitioning to the parent company's CIP compliance program.

ReliabilityFirst determined the duration of the violation to be from when the individual was improperly granted access to the PSP, through when URE2 completed its Mitigation Plan.

URE2 submitted its Mitigation Plan designated RFCMIT011397 to address the referenced violations. URE2's Mitigation Plan required URE2 to consolidate access requests into a single system requiring verification of credentials before commissioning.

URE2 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE2 had completed all mitigation activities.

RFC2014013802 CIP-005-3a R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R1 by failing to: a) identify and document all access points to the perimeter(s); b) identify and protect one or more noncritical Cyber Assets within a defined ESP to the requirements of Standard CIP-005, c) afford Cyber Assets used in the access control and/or monitoring of the ESP(s) one or more of the required protective measures of R1.5; and d) maintain documentation of some interconnected critical and noncritical Cyber Assets within the ESP(s), electronic access points to the ESP(s), and Cyber Assets deployed for the access control and monitoring of these access points.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to identify and adequately protect the ESP, as well as all access points on the ESP, could have led to serious harm to the BPS by increasing the likelihood that cyber intrusions could have occurred resulting in damage to various critical and noncritical Cyber Assets.

The risk posed by the foregoing facts and circumstances was partially mitigated by the following factors. First, all currently identified CCAs reside within a defined ESP, and the subsidiary had measures in place to protect and restrict access to the ESP and physical access to the devices themselves. Specifically, the subsidiary had electronic logging to monitor access to the ESPs, password protections on the connections to the network systems, and other protective measures including intrusion detection and anti-malware. Furthermore, physical access to the ESP devices was highly restricted to appropriate personnel with multiple physical access control layers within a non-public, controlled space. The ESP devices are in a secured facility, under constant surveillance, and are located in a secured data center, which provides an attestation of the controls environment, and the backup GMS is located in a secured room. All doorways to the secured rooms at each location are alarmed for forced entry and monitored with cameras. Additionally, the electronic access control and monitoring devices were protected by the subsidiary's cyber security policies and procedures, and the people accessing those devices had received cyber security training and have PRAs on file. Finally, although not all assets were listed on the ESP documentation, documentation of the ESP and related assets exists in multiple forms such as a Visio diagram and asset lists.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011319 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-005 compliance program and perform a preliminary ESP and electronic access point design to ensure that every CCA resides within an ESP and that the ESP and all access points to it have been properly identified and documented;
2. validate the new configuration to ensure that all CCAs and access points are properly identified and documented; and
3. train all appropriate personnel on the actions necessary for compliance with CIP-005-3a R1.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013803 CIP-005-3a R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R2 by failing to: a) document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs; b) use an access control model with respect to its processes and mechanisms that denies access by default, such that explicit access permissions must be specified; c) ensure that, at one or more access points to the ESPs, only ports and services required for operations and for monitoring Cyber Assets within the ESP were enabled, or document, individually or by specified grouping, the configuration of those ports and services; d) implement strong procedural or technical controls at the access points where external interactive access into the ESP had been enabled, to ensure authenticity of the accessing party, where technically feasible; and e) maintain all appropriate documentation.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to formally implement and document the organizational processes and technical and procedural mechanisms in place to control electronic access to the ESPs could have led to serious harm to the BPS by increasing the likelihood that cyber intrusions could have occurred resulting in damage to various critical and noncritical Cyber Assets. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011316 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-005 Compliance Program and associated procedures for URE1's Cyber Assets to perform a preliminary network design of electronic access control and monitoring (EACM) of ESP access points;
2. identify technical and procedural mechanisms for electronic access control and monitoring of ESP access points as part of the electronic access controls program re-design change control process;
3. implement the resulting new configuration to ensure that all technical and procedural EACMs at ESP access points are documented and in place; and
4. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013804 CIP-005-3a R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R3 by failing to document electronic or manual processes for monitoring and logging access points to the ESPs twenty-four hours per day, seven days per week. Also, even though technically feasible, the subsidiary failed to implement security monitoring processes to detect and alert for attempted or actual unauthorized accesses. Rather, the subsidiary relied on manual review of generated logs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of formal, documented electronic or manual processes for monitoring and logging access points to the ESPs poses a serious risk to the reliability of the BES because it increases the likelihood that an individual could obtain unauthorized access to the ESP without leaving any record of the intrusion.

The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although undocumented, the subsidiary utilized manual processes for monitoring and logging access at access points to the ESPs twenty-four hours per day, seven days per week. Specifically, the subsidiary utilized an intrusion detection program, among other tools, to monitor and log access. The resulting logs of attempted or actual unauthorized accesses were reviewed at least every 90 calendar days.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011317 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the parent company's EMS integrated system change control and commissioning process, identify systems for continuous monitoring and logging of access at ESP access points, as well as protocols for receiving alerts and alarm response;
2. utilize the parent company's NERC CIP-005 compliance program and associated procedures to design technical controls for access monitoring, logging, and alerting at ESP access points;
3. implement and documenting the new configuration to ensure that monitoring and logging of ESP access points is taking place and that alerting and alarm response protocols are enabled; and
4. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013805 CIP-005-3a R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-005-3a R4 by failing to perform a Cyber Vulnerability Assessment (CVA) at least annually for one or more of the access points to the ESPs, and the CVA, once performed, did not include one or more of the sub-requirements of R4. Specifically, some devices were not included in the CVA, and the CVA did not include an action plan to remediate or mitigate vulnerabilities identified during the CVA and the execution status of that plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to perform a CVA prevented the subsidiary from identifying inherent vulnerabilities associated with its CCAs. Allowing such vulnerabilities to remain unknown increases the risk that an individual could gain unauthorized access to CCAs within the ESP and cause harm to the integrity of the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011312 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. perform a CVA in accordance with the required vulnerability assessment process, review and verify that only ports and services required for operations at these access points are enabled, review controls for default accounts, and document the results of the CVA;
2. develop an action plan for the CVA and document the execution status of that action plan;
3. utilize the parent company's NERC CIP-005 Compliance Program and associated procedures for the EMS integrated system to gather the required information for the CVA;
4. define the scope of work for the CVA that is required; and
5. train appropriate personnel on the actions necessary for compliance with CIP-005-3a R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013833 CIP-005-3a R5- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-005-3a R5 by failing to formally define the documentation that would be required for compliance with CIP-005-3. Therefore, the subsidiary failed to review, update, and maintain any such documentation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation is a documentation issue. ReliabilityFirst also notes that the subsidiary identified no known instances where a change to the network or controls was made that would have necessitated a corresponding change in documentation because only minimal system hardware or software changes occurred during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011304 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security ESP Program for CIP-005-3a;

2. implement a process of formal review and attestation of review for the cyber security ESP Program to ensure that documentation is updated to reflect a modification of the network controls within 90 calendar days of the change; and
3. have a committee to create an attestation of review for ongoing process improvement for CIP-005-3a compliance.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013810 CIP-006-3c R1- OVERVIEW

ReliabilityFirst determined that the subsidiary violated CIP-006-3c R1 by failing to ensure that its physical security plan: a) addressed and included processes to ensure and document that all Cyber Assets within an ESP also reside within an identified PSP; b) identified all access points through each PSP; c) included processes, tools, and procedures to monitor physical access to the perimeter(s); d) addressed the appropriate use of physical access controls as described in R4; and e) met the requirements of continuous escorted access of visitors within the PSP. Moreover, the current physical security perimeter plan failed to accurately identify the PSP. The plan identified the PSP inaccurately as the room in which the GMS sits, rather than the more appropriate identification of the PSP as the cabinet in which the currently identified CCAs reside.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although the subsidiary's documentation lacked many elements required by CIP-006-3c R1, it had a physical security plan that addressed the identification of a PSP, protection of Physical Access Control Systems (PACS), protection of electronic access controls systems, physical access controls, monitoring physical access, logging physical access, access log retention, and maintenance and testing related to the PACS identified in the plan. Second, while a true "six-wall border" was not in place, physical access to all currently identified CCAs was highly restricted.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011230 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-006 Compliance Program to design new PSPs for physical protection of CCAs and associated controls;
2. build new PSPs and implement appropriate controls;

3. revise the parent company's physical security plan documentation to include URE1's physical access controls; and
4. train appropriate personnel the design, implementation, and maintenance of the new physical security plan.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2015014715 CIP-006-3c R1- OVERVIEW

ReliabilityFirst determined that URE2 violated CIP-006-3c R1 by allowing an unauthorized cleaning contractor to access a PSP without an escort at URE2. The first instance of this violation occurred when an authorized contractor swapped his daily cleaning duties with an unauthorized coworker. In doing so, the authorized contractor passed his access badge to the unauthorized cleaning contractor, enabling the contractor to gain access into the side door of the PSP for a total of five hours. The second instance of this violation occurred over the course of six days. In this instance, the same authorized contractor was preparing to leave for vacation and passed his access badge to an unauthorized contractor, enabling that unauthorized individual to gain access to a PSP without an escort for a total of six hours. In both instances, the use of the authorized swapped badge was detected by a shift supervisor or facilities management and the unauthorized personnel were removed from the PSP. Also, in both instances, the authorized contractor who swapped his badge did not understand the restrictions around sharing his badge with unauthorized personnel and the unauthorized contractors did not follow proper protocol for obtaining a continuous escort while accessing the PSP.

Review of the PSP and CCAs indicates that there was no compromise of assets and incident review with the contractors indicates that there was no malicious intent on the part of the authorized contractor, nor the unescorted visitors. In addition, in each of these circumstances, a current parent company authorized party was present within the PSP.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, URE2 was aware whenever the cleaning crew was within the PSP. Second, authorized personnel were present within the PSP each time that an unauthorized cleaning contractor was present. ReliabilityFirst also notes that, as stated above, a review of the PSP and CCAs indicates that there was no compromise of assets and incident review with the contractors indicates that there was no malicious intent on the part of the authorized contractor, nor the unescorted visitors.

ReliabilityFirst determined the duration of the violation to be from when the first unauthorized contractor was granted access to the PSP, through the last date on which an unauthorized contractor accessed the PSP.

URE2 submitted its Mitigation Plan designated RFCMIT011508 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. conduct an incident review with management for the cleaning contracting company;
2. evaluate alternate cleaning contract company sourcing;
3. make a sourcing contract change;
4. conduct PRAs and training for three new cleaning personnel; and
5. review physical access escorting protocol with new contractor management.

RFC2014013811 CIP-006-3c R2- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-006-3c R2 by failing to afford the protective measures specified in CIP-003-3, CIP-004-3 R3, CIP-005-3 R2 and 3, CIP-006-3 R4 and 5, CIP-007-3, CIP-008-3, and CIP-009-3 for all Cyber Assets that authorize and/or log access to the PSPs, such as electronic lock mechanisms and badge readers.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. First, although the PACS were not afforded all of the required protections, they were protected by a corporate security standard that included limited access, both physically and logically, and utilized antivirus and antimalware tools. Second, the PACS are on isolated networks and are independent of the ESPs containing CCAs. Therefore, unauthorized electronic access to PACS devices would not, in itself, lead to the compromise of CCAs or other Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011223 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. design and identifying new PACS to be used for change control and configuration planning;
2. implement the new PACS and ensure appropriate controls are applied;
3. revise the parent company's PSP program documents to include URE1's PACS; and

4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013812 CIP-006-3c R3- OVERVIEW

ReliabilityFirst determined that URE1 violated CIP-006-3c R3 by failing to properly identify a formal PSP within which Cyber Assets used in the access control and/or monitoring of the ESPs reside. URE1 incorrectly identified its PSP, thus resulting in the corresponding violation of CIP-006-3c R3.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although URE1 did not have a properly identified PSP, the physical security mechanisms were in place and applied to the Cyber Assets responsible for the access control and/or monitoring of the ESPs. Thus, the likelihood that an individual could have gained unauthorized physical access to the Cyber Assets within the PSP was low.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011231 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. ensure that newly identified EACMS will be protected within a PSP as part of the PSP re-designs for change control planning;
2. implement new EACMS and ensure appropriate PSP and PACS controls are applied;
3. revise the parent company's PSP documents to include URE1's EACMS; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013809 CIP-006-3c R3- OVERVIEW

ReliabilityFirst determined that URE4 violated CIP-006-3c R3 by permitting a Cyber Asset used in the access control and/or monitoring of the ESP to reside outside of an identified PSP. Specifically, URE4 had a firewall contained within a communications room, but not within a declared PSP.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the firewall was afforded protection under CIP-005 R1.5 except being protected within a PSP. Second, the area where the firewall resides is located in an interior part of the administration building which is key-locked and not available to the general public. Third, the firewall was further protected by restricted access to each overall facility including, but not limited to, guard service, perimeter fencing, and operator rounds checking for intrusion. ReliabilityFirst also notes that logs for the system monitoring this device did not show evidence of ESP activity resulting from physical intrusions during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE4 completed its Mitigation Plan.

URE4 submitted its Mitigation Plan designated RFCMIT011438-1 to address the referenced violations. URE4's Mitigation Plan required URE4 to:

1. implement and commission a new PACS;
2. reconfigure its Cyber Assets so that they are protected within a PSP; and
3. update the PSP documentation to reflect the new configuration.

RFC2014013813 CIP-006-3c R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R4 by failing to document the operational and procedural controls to manage physical access at all access points to the PSP(s) twenty-four hours a day, seven days a week using one or more of the following physical access methods: card key, special locks, security personnel, or other authentication devices such as biometric, keypad, token, or other equivalent devices that control physical access to the CCAs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the requisite operational and procedural controls were not properly documented, URE1 had many of them in place including the use of card keys, man trap systems, cyber locks, security personnel responsible for controlling physical access, biometric readers, and keypads. Accordingly, URE1 had multiple physical access control layers within a nonpublic, controlled space which was under constant surveillance.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011232 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop formal documentation of the physical security plan which contains the operation and procedural controls to manage physical access at all access points to the PSP as required by CIP-006-3c.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013814 CIP-006-3c R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R5 by failing to document or implement the technical and procedural controls for monitoring physical access at all access points to the PSP(s) twenty-four hours a day, seven days a week using one or more of alarm systems or human observation of access points. Specifically, alarm systems or human observation specific to the restricted access cabinet (representing the PSPs) were not addressed.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Although alarming or human observation was not in place specifically related to the cabinets containing the CCAs, these (and the other physical access tools) were in place to restrict physical access. These additional protections reduced the likelihood that an individual could have gained unauthorized access to the PSP

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011233 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the PSP re-design, ensure that all PSP physical access points will have appropriate technical and procedural controls for access monitoring twenty-four hours per day, seven days per week;
2. implement new PACS equipment and processes for monitoring PSP physical access points;
3. revise the current parent company's physical security plan documents to include URE1's physical access controls monitoring; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R5.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013815 CIP-006-3c R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R6 by failing to implement or document the technical and procedural mechanisms for logging physical entry at all access points to the PSP(s) using one or more of the following logging methods or their equivalent: computerized logging, video recording, or manual logging. Specifically, logging of the physical access to the cabinet representing the PSPs was not addressed.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although they were undocumented, URE1 had several technical and procedural mechanisms in place for logging physical entry at all access points to the PSPs including the use of cyber lock access logs, card reader access logs, manual logs, biometric and keypad logs, and a video log of access. Accordingly, URE1 had multiple physical access logging layers of access to a restricted non-public, controlled space containing the locked cabinets and logs related to the access of the cabinets themselves.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011219 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal physical security plan process to include documentation of the technical and procedural mechanisms for logging physical entry at all access points to the PSPs in compliance with CIP-006-3c.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013834 CIP-006-3c R7- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R7 by failing to retain physical access logs for at least ninety days. Specifically, the subsidiary failed to retain logs for physical access to the locked cabinets containing CCAs.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although logs were not retained for ninety days for the locked cabinet representing the PSP, the subsidiary had other mechanisms in place for logging physical entry at all access points to the PSPs include the use of card reader logs, manual logs, biometric scan and keypad logs, and video log of access. Logs generated via these mechanisms were retained for 90 days as a matter of policy.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011220 to address the referenced violations. URE1's Mitigation Plan required URE1 to implement the cyber lock system, which provided the ability to log physical access to the locked cabinets, and to maintain those logs for 90 calendar days.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013835 CIP-006-3c R8- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-006-3c R8 by failing to have a formal, documented physical security plan that contained a maintenance and testing program.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The former subsidiary implemented a maintenance and testing program within the three-year cycle called for in CIP-006-3c R8. However, that program was not fully adequate because it did not address all of the components required by CIP-006-3c R8. Nevertheless, the tests verified that the risk was minimal, as several physical security mechanisms were in place prior the documentation of the testing program, which secured the PSP.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011224 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. as part of the PSP re-design, ensure that all new PACS and physical security systems will have appropriate maintenance and testing programs;
2. ensure that its physical security plan includes testing and maintenance schedules for associated physical security system and physical access controls to ensure proper functioning;
3. ensure that the current parent company's physical maintenance and testing program includes updated documentation for the new URE1's PSP, retention of access controls outage records, logging and monitoring; and
4. train appropriate personnel on the actions necessary for compliance with CIP-006-3c R8.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013820 CIP-007-3a R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R1 by failing to document the cyber security test procedures necessary to minimize the effects of changes to the production environment. Moreover, the subsidiary failed to: a) perform testing for all changes that met the definition of "significant" contained in CIP-007-3a R1; and b) document that testing was done in a manner that reflects the production environment. Finally, the subsidiary retained documentation for some changes, but inaccurately determined that testing was not necessary.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of documented cyber security test procedures increases the likelihood that the subsidiary could introduce new Cyber Assets to the ESP or make significant changes to existing Cyber Assets within the ESP without knowledge of potential adverse effects to the subsidiary's cyber security controls changes. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The subsidiary had an informal change management process in place that utilized a ticketing system to approve and track master change requests for all changes to currently identified CCAs. This process included the documentation of testing, when the subsidiary deemed testing to be appropriate.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011311 to address the referenced violations. URE1's Mitigation Plan required URE1 to develop a formal, documented cyber security testing program necessary to minimize the effects of changes to the production environment, and to train all responsible individuals on the cyber security testing program and revised procedures to ensure ongoing security.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013821 CIP-007-3a R2- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R2 by failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled. Also, the subsidiary: a) enabled one or more ports or services not required for

normal and emergency operations on Cyber Assets inside the ESP; b) did not disable one or more other ports or services, including those used for testing purposes, prior to production use for Cyber Assets inside the ESP; and c) for cases where unused ports and services cannot be disabled due to technical limitations, did not document compensating measure(s) applied to mitigate risk.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. This failure increased the likelihood of infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. This type of infiltration could cause significant harm to URE1's CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011310 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures of URE1's Cyber Assets, ensuring that (change control) commissioning design of ports and services configuration includes processes to: a) baseline ports and services; b) disable unneeded ports and services; and c) properly justify all enabled ports and services;
2. initially document baseline ports and service targets and justifications;
3. implement baseline process to align URE1's ports and services with compliance program documentation; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R2.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2015015243 CIP-007-3a R3- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R3 by: a) failing to implement or document, either separately or as a component of the documented configuration management process specified in CIP-003-3 R6, a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP(s); b) failing to document the assessment of security patches and security upgrades for applicability as required in Requirement R3 within 30 calendar days after the availability of the patches and upgrades;

c) failing to document the implementation of applicable security patches as required in R3 or where an applicable patch was not installed; and d) failing to document the compensating measure(s) applied to mitigate risk.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The installation of untested patches can result in computers and servers crashing, creating a reliability issue. Moreover, the failure to test or monitor patches could create windows of opportunity to compromise the system.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted Mitigation Activities to address the referenced violations. URE1's Mitigating Activities represented that URE1:

1. utilized the current parent company's NERC CIP-007 Compliance Program to design patch management for newly identified Cyber Assets;
2. identified security patch sources;
3. implemented security patch management process; and
4. trained appropriate personnel on the process.

RFC2014013795 CIP-007-3a R3- OVERVIEW

ReliabilityFirst determined that URE2 violated CIP-007-3a R3 by failing to perform patch assessments for third-party applications after commissioning the EMS system. Although the responsible individual was performing operating system level patches at proper intervals based on scheduled tasks, he was unaware of his responsibility to assess third-party patches, which are separate and distinct from those related to the operating system.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The risk was increased due to the EMS being involved in the violation, which increased the risk that the EMS could have been exploited via a vulnerability resulting from an unassessed patch. Furthermore, ReliabilityFirst noted that this violation was not the result of URE2 simply failing to assess two third-party application patches while performing assessments on all other third-party application patches. Rather, this violation was the result of URE2's general lack of awareness to assess third-party application patches.

Nevertheless, ReliabilityFirst notes that the risk posed by this violation was mitigated by the following factors. First, only two security-related patch updates were missed during the period of the violation. Second, all of the operating system level patch assessments for all applicable devices were performed during the period of the violation.

ReliabilityFirst determined the duration of the violation to be from the date that the first third-party patches were not assessed, through when URE2 completed its Mitigation Plan.

URE2 submitted its Mitigation Plan designated RFCMIT011437 to address the referenced violations. URE2's Mitigation Plan required URE2 to provide additional training for responsible personnel on patch assessment requirements.

RFC2014013822 CIP-007-3a R4- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R4 by failing to document the implementation of antivirus and malware prevention tools for cyber assets within the ESP. Moreover, the subsidiary failed to implement a process which addressed testing and installing the signatures for the update of antivirus and malware prevention "signatures."

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The subsidiary's failure to document its anti-virus and malware prevention tools increases the likelihood that it would be unaware of what type or version of these tools it was running. This lack of awareness could result in serious vulnerabilities to subsidiary's cyber security system. The risk posed by the foregoing facts and circumstances was mitigated by the fact that subsidiary had been using undocumented antivirus software and other malware prevention tools for all Cyber Assets within the ESP.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011309 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets to design configuration of tools to: a) test antivirus signatures prior to roll-out; and b) install antivirus signatures on all applicable Cyber Assets;
2. identify all applicable Cyber Assets for installation of antivirus signatures;

3. ensure that antivirus software has been installed on all applicable Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R4.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013823 CIP-007-3a R5- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R5 by failing to: a) document technical and procedural controls that enforce access authentication of, and accountability for, all user activity; b) ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed; c) have designated personnel approve one or more user accounts implemented by the subsidiary; d) review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003-3 Requirement R5 and Standard CIP-004-3 Requirement R4; e) implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts; f) for accounts that must remain enabled, change passwords prior to putting any system into service; g) identify all individuals with access to shared accounts; h) where such accounts must be shared, implement (one or more components of) a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination); and i) require passwords subject to R5.3.2 and R5.3.3.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of adequate controls to meet the requirements of CIP-007-3a R5 increases the likelihood that an individual could gain unauthorized access system access and cause serious damage. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011308 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the current parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets, ensuring that configuration management planning includes processes to: a) baseline all accounts (admin,

shared, service accounts, and generic accounts); b) disable default accounts or change default passwords; c) verify password complexity requirements are met; d) validate access privileges for individuals on the updated CCA access list; and e) ensure traceability of user activity on applicable Cyber Assets;

2. perform initial documentation of its baseline targets for items a) through e) above;
3. implement the parent company's account management process to document account updates for addition of URE1's Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R5.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014014469, RFC2014013797, RFC2014013816 CIP-07-3a R5, R5.2.3- OVERVIEW

RFC2014014469

ReliabilityFirst determined that URE2 failed to provide sufficient, or appropriate, evidence to support a valid audit trail of shared, generic, or administrative accounts for the Windows environment. Although URE2 produced sufficient evidence as to who was using generic or shared accounts for other environments (e.g., operating systems and networking devices), URE2 failed to produce any electronic or manual records demonstrating who used the shared or generic account in the operating system environment.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE2 has several procedural controls in place including the current parent company's procedure for acceptable use and definition of the parent's shared accounts, as well as system logs and reviews to track and review when a generic or shared account is used and who has access to use those accounts. Thus, the potential risk associated with not being able to identify which individual is actually using one of these accounts at any given time is minimal.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE2 completed its Mitigation Plan.

URE2 submitted its Mitigation Plan designated RFCMIT011337 to address the referenced violations. URE2's Mitigation Plan required URE2 to:

1. modify the existing CIP-007 R5 procedure to address appropriate administrative level operating system shared accounts use;

2. modify the CIP-007 R5 training for account use specific to administrator level shared account use and record privileged account users attendance; and
3. implement technical or manual logging of administrative level operating system shared accounts, including an alerting feature for system logging.

RFC2014013797

ReliabilityFirst determined that URE3 violated CIP-007-3a R5 by failing to ensure that all individual and shared system account passwords are changed at least annually. Specifically, the passwords for two service accounts were older than 365 days.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, the affected accounts were known to be disabled for interactive login, which reduces the likelihood that these accounts could be compromised. Second, the device at issue is a Cyber Asset for a small group of facilities which rarely run. ReliabilityFirst also notes that an initial evaluation by URE3 indicated that the affected accounts had not been used since creation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE3 completed its Mitigation Plan.

URE3 submitted its Mitigation Plan designated RFCMIT011424-1 to address the referenced violations. URE3's Mitigation Plan required URE3 to:

1. implement the current parent company's CIP-007 account management procedure to manage built-in accounts when needed;
2. deploy automated scripts to check for passwords nearing the age threshold, verify system password complexity settings and send a report to the site gate keeper; and
3. submit a Technical Feasibility Exception (TFE) for the two system accounts at issue.

RFC2014013816

ReliabilityFirst determined that URE4 violated CIP-007-3a R5 by failing to ensure that all individual and shared system account passwords are changed at least annually. Specifically, three enabled operating system user accounts were found to have passwords older than 365 days.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. First, even though the passwords were not changed in over 365 days, URE4 had other controls in place to physically and logically protect these accounts and devices. Specifically,

these devices resided within an ESP and PSP. Additionally, URE4 generated logs for these devices and accounts to track who accessed them. Second, the devices at issue are Cyber Assets for a small group of facilities which rarely run. ReliabilityFirst also notes that an initial evaluation by URE4 indicated that the affected accounts had been rarely used since their creation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE4 completed its Mitigation Plan.

URE4 submitted its Mitigation Plan designated RFCMIT011439-1 to address the referenced violations. URE4's Mitigation Plan required URE4 to:

1. implement the current parent company's CIP-007 account management procedure to manage built-in accounts when needed;
2. disable the built-in accounts and then test the functionality of the application; and
3. deploy automated scripts to check for passwords nearing the age threshold, verify system password complexity settings and send a report to the site gate keeper.

RFC2014013824 CIP-007-3a R6- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R6 by failing to: a) implement automated tools or organizational process controls, as technically feasible, to monitor system events that are related to cyber security on one or more of Cyber Assets inside the ESP in that some of the CCAs within the ESP were missing logs and not all devices within the ESP were accounted for; b) implement and document the organizational processes and technical and procedural mechanisms for monitoring security events on all Cyber Assets within the ESP in that the subsidiary's security monitoring controls do not issue automated or manual alerts for detected cyber security incidents; c) maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008; d) retain one or more of the logs specified in Requirement R6 for at least 90 calendar days without obtaining TFEs for devices that cannot log events; and e) review logs of system events related to cyber security nor maintain records documenting review of logs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The lack of automated tools or organizational process controls to monitor system events that are related to cyber security increases the likelihood that undetected compromise of CCAs and other system events that are related to cyber security could occur without the subsidiary's knowledge.

The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although the subsidiary failed to monitor all devices within the ESP for unauthorized cyber or physical access, the GMS, backup GMS, and firewalls were being monitored. Moreover, all Cyber Assets related to the primary and backup GMS were protected by the logical and physical access controls

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011307 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. utilize the parent company's NERC CIP-007 compliance program and associated procedures for change control and commissioning of URE1's Cyber Assets, ensuring that program includes a) processes to monitor all applicable Cyber Assets, including EACMS and PACS; and b) alerting and investigation processes for URE1's Cyber Assets;
2. identify applicable Cyber Assets for security status monitoring, alerting and logging, and to document TFEs as necessary;
3. ensure that security status monitoring, alerting, and log review will be documented and enabled for applicable Cyber Assets; and
4. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R6.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013915 CIP-007-3a R7- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R7 by failing to document the operation and procedural controls to manage the disposal or redeployment of CCAs within the ESP.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The relatively short duration of this violation minimized the likelihood that any data from Cyber Assets could have been retrieved by an unauthorized individual. In addition, URE1 created a technical instruction checklist for disposal of Cyber Assets containing protected cyber information. Furthermore, URE1 does not redeploy Cyber Assets that have been inside the ESPs.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011315 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. define the cyber security systems management plan containing operational and procedural controls to manage the disposal or deployment of Cyber Assets within the ESP;
2. implement the cyber security systems management plan; and
3. develop formal documentation of the cyber security systems management plan containing operation and procedural controls to manage the disposal or deployment of Cyber Assets within the ESP and technical instruction for its execution.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013825 CIP-007-3a R8- OVERVIEW

ReliabilityFirst determined that prior to being acquired by the current parent company, the former subsidiary violated CIP-007-3a R8 by failing to perform a CVA, at least annually, of all Cyber Assets within the ESP. An initial CVA did not address all of the sub-requirements of CIP-007-3a R8. Specifically, some devices were not included in the scope of the CVA, and the CVA did not include an action plan to remediate or mitigate vulnerabilities identifying during the CVA and the execution status of that action plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The failure to perform a CVA prevented the former subsidiary from identifying inherent vulnerabilities associated with its CCAs. Allowing such vulnerabilities to remain unknown increased the risk that an individual could gain unauthorized access to CCAs within the ESP and caused harm to the integrity of the CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the logical and physical access controls.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011318 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. perform a CVA in accordance with the required vulnerability assessment process, review and verify that only ports and services required for operations at these access points are enabled, review controls for default accounts, and document the results of the CVA;

2. develop an action plan for the CVA and document the execution status of that action plan;
3. utilize the current parent company NERC CIP-007 Compliance Program and associated procedures to gather the required information for the CVA;
4. define the scope of work for the CVA that is required to be completed by the end of 2015; and
5. train appropriate personnel on the actions necessary for compliance with CIP-007-3a R8.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013836 CIP-007-3a R9- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-007-3a R9 by failing to formally define the documentation that would be required for compliance with CIP-007-3. Thus, the subsidiary failed to review, update, or maintain any such documentation.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation is a documentation issue. ReliabilityFirst also notes that URE1 identified no known instances where a change to the network or controls was made that would have necessitated a corresponding change in documentation because only minimal system hardware or software changes occurred during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011313 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the cyber security systems management program for CIP-007-3a; and
2. implement a formal review and attestation process to ensure that the documentation is updated, reviewed, and maintained to reflect modifications to the systems, configurations, or controls within 30 days of the change.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013826 CIP-008-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-008-3 R1 by failing to document or formally develop a cyber security incident response plan that addressed all of the requisite items. However, the subsidiary had an informal process in place for reporting cyber security incidents, but that informal process lacked the requirements of CIP-008-3 R1.1, 1.2, and 1.6.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk was mitigated because URE1 had an informal process in place for reporting cyber security incidents. ReliabilityFirst also notes that no cyber security incidents occurred during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011217 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. develop formal documentation of the measures in place for classifying events, roles and responsibilities for response actions, process for reporting, updating, and ensuring the cyber security incident response plan meets the requirements of CIP-008-3 R1; and
2. formally adopt the cyber security incident response plan for CIP-008-3.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

RFC2014013827 CIP-009-3 R1- OVERVIEW

ReliabilityFirst determined that the former subsidiary violated CIP-009-3 R1 by failing to create a recovery plan for CCAs. Rather, the subsidiary only had an informal, undocumented process in place for the recovery of CCAs.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The lack of a formal, documented recovery plan increases the likelihood that the subsidiary would be unable to recover any failed CCAs. The risk posed by the foregoing facts and circumstances was mitigated by the fact that the subsidiary had an informal, undocumented process in place to recover failed CCAs. ReliabilityFirst also notes that no CCA outages occurred during the period of this violation.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE1 completed its Mitigation Plan.

URE1 submitted its Mitigation Plan designated RFCMIT011227 to address the referenced violations. URE1's Mitigation Plan required URE1 to:

1. implement the recovery plan for CCAs as called for by CIP-009-3 R1;
2. develop formal documentation of the recovery plan for CCAs which will contain required actions in response to events and defined roles and responsibilities.

URE1 certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE1 had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one hundred and fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered the URE Entities' compliance history as an aggravating factor in the penalty determination;
2. the URE Entities had an internal compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor;
3. the URE Entities self-reported 12 of the violations, and ReliabilityFirst applied some mitigating credit;
4. ReliabilityFirst received a number of the violations as a result of the mandatory Self-Certification process, thus ReliabilityFirst did not provide mitigating credit for the violations during this process;
5. URE1 implemented tools and other measures to enhance the security and reliability of its systems beyond that which is required by the CIP Reliability Standards. ReliabilityFirst has awarded mitigating credit for these measures;
6. the URE Entities were highly cooperative throughout the compliance enforcement process;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. ReliabilityFirst considered the risk and harm posed by the URE Entities to the reliability of the BPS as serious or substantial in the aggregate; and

9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred and fifty thousand dollars ($150,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 16, 2015 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and fifty thousand dollars ($150,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0682 (216) 503-9207 facsimile bob.wargo@rfirst.org Deandra Williams-Lewis* Director of Enforcement ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0689 (216) 503-9207 facsimile deandra.williamslewis@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0683 (216) 503-9207 facsimile jason.blake@rfirst.org	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Patrick O'Connor* Associate Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 (216) 503-0668 (216) 503-9207 facsimile patrick.oconnor@rfirst.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entities
ReliabilityFirst

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

February 29, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[1] with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of violations of NERC CIP Reliability Standards.

According to the Settlement Agreement, URE stipulates to the facts included in the Settlement Agreement and admits that these facts may constitute violations. URE has agreed to the assessed penalty of one million seven hundred thousand dollars ($1,700,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between ReliabilityFirst and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the

[1] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2014014245	CIP-002-3	R3	CA	Moderate	$1,700,000
RFC2014014014	CIP-003-1	R6	SR	Serious	
RFC2014014251	CIP-004-3	R2	CA	Moderate	
RFC2014014252	CIP-004-3	R2.1		Serious	
RFC2014014253	CIP-004-3	R3.3		Moderate	
RFC2013013197	CIP-004-3a	R4.2	SR		
RFC2014013447	CIP-004-3a	R4.2	SR		
RFC2014013997	CIP-004-3a	R4.2	SR		
RFC2014013623	CIP-005-1	R1.5	SR	Serious	
RFC2014014015	CIP-005-3a	R1.5	SR	Minimal	
RFC2014014207	CIP-005-3	R1.6	CA	Serious	
RFC2015015300	CIP-005-3a	R1			
RFC2014014410	CIP-006-3c	R1	SR	Minimal	
RFC2014014011	CIP-006-1	R1.1	SR	Moderate	

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2014014208	CIP-006-3a	R1.8	CA	Moderate	$1,700,000
RFC2015015143	CIP-006-3a	R1	SR		
RFC2014014209	CIP-006-3a	R5	CA	Serious	
RFC2013013198	CIP-006-3c	R5	SR		
RFC2014014211	CIP-007-3a	R1.3	CA		
RFC2014013998	CIP-007-1	R2	SR		
RFC2014013626	CIP-007-1	R3	SR		
RFC2014014262	CIP-007-3a	R3, R3.1, R3.2	SR		
RFC2014014114	CIP-007-3a	R3.2			
RFC2014014012	CIP-007-3a	R4	SR	Minimal	
RFC2014014215	CIP-007-3a	R5.1.2	CA		
RFC2014014216	CIP-007-1	R5.2, R5.2.3		Serious	
RFC2014014257	CIP-007-3a	R5.3; R5.3.1, R5.3.2, R5.3.3			
RFC2014014238	CIP-007-3a	R9	CA	Moderate	
RFC2014014239	CIP-008-3	R1.6			
RFC2014014240	CIP-009-3	R1		Serious	
RFC2014014241	CIP-009-3	R2			

NERC Violation ID	Standard	Req	Discovery Method* Date	Risk	Penalty Amount
RFC2015015301	CIP-009-3	R2		Serious	$1,700,000
RFC2014014013	CIP-009-1	R4	SR		
RFC2015015302	CIP-009-3	R4			
RFC2014014242	CIP-009-3	R5	CA		
RFC2015015303	CIP-009-3	R5			

Background

During a Compliance Audit and subsequent enforcement process, ReliabilityFirst determined that URE had serious, systemic security and compliance issues across URE's multiple business units. Additionally, multiple violations were repeats of prior violations. Some of the most significant violations involved patching and physical security. For example, regarding patching under CIP-007-3a R3, URE did not patch its energy management system (EMS) after it completed its mitigation plan for the same violation identified during a previous CIP Compliance Audit. In another example, regarding physical security, URE discovered that three Physical Security Perimeter (PSP) doors to a central control room had been tampered with, presumably by employees, thus preventing the doors from latching securely. URE's most recent issue with securing its PSP occurred when an employee worked eight shifts despite URE revoking the employee's physical access for failure to complete annual requalification training. Of the 36 violations, ReliabilityFirst determined that 21 violations posed a serious and substantial risk to the reliability of the Bulk Power System (BPS), 11 posed a moderate risk to the reliability of the BPS, and the remaining 4 posed a minimal risk to the reliability of the BPS. ReliabilityFirst considered the risk and harm posed by the violations to the reliability of the BPS in the aggregate and determined that these violations collectively posed a serious and substantial risk to the reliability of the BPS.

The root causes of these violations were cultural issues that resulted in URE management's lack of awareness, engagement, and accountability for CIP compliance. Moreover, URE failed to identify its CIP issues, and even after identification, failed to promptly address the CIP issues. URE delayed submitting Mitigation Plans, was late in completing many of its Mitigation Plans, and failed to complete four Mitigation Plans, which resulted in ReliabilityFirst requiring URE to prepare and submit 4 new Mitigation Plans.

ReliabilityFirst notes that URE has recently agreed to work with ReliabilityFirst through at least the second quarter of 2016 to holistically evaluate and work to improve its culture and thus its overall security posture and CIP Compliance Program. URE has committed to ReliabilityFirst that improvements will include increased senior management involvement, reorganization, increased resources, and significant process improvements.

RFC2014014245 CIP-002-3 R3 - OVERVIEW

ReliabilityFirst determined that URE did not provide sufficient evidence of identifying programmable relays as Cyber Assets and URE failed to identify several Critical Assets correctly. First, two switches located at a backup control center were listed by URE as access points, but were actually Critical Cyber Assets (CCAs) and not access points. Second, a server was identified by URE as a CCA, but based on URE's methodology, should have been identified as a non-CCA. Third, a CCA listed on URE's list of CCAs was identified during a site visit of the Compliance Audit, but was not included on URE's pre-audit submission of identified Cyber Assets. In addition, ReliabilityFirst determined that URE did not provide evidence demonstrating an adequate evaluation of programmable relays for CCA identification. This determination was based on a lack of information on URE's pre-audit submissions and subsequent lack of clarity from subject matter expert interviews on the same subject.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not developing a complete lists of CCAs increased the risk that URE would miss CCAs that were not on the list when implementing the security controls. URE exhibited a lack of processes and procedures to ensure the reliable identification of those devices that are critical. Such process and procedure gaps result in violations that are likely to be repeated. The risk was only partially mitigated because not all of the devices were determined to be CCAs, and were therefore less critical to security.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011422 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its process for annually reviewing, documenting, and determining whether programmable relays for protective systems are CCAs;
2. update and implement its asset validation process to include validating the classification of each asset on the list of Cyber Assets and to include a review of the entire list of assets to verify each asset has been classified and evaluated correctly; and

3. design an internal pre-specification for completing the Attachment C, which is an input to the pre-audit process for ReliabilityFirst.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014014 CIP-003-1 R6 - OVERVIEW

ReliabilityFirst determined that URE retained an independent vendor to perform a NERC CIP gap analysis, which revealed that URE's process for requesting changes to firewall rules failed to include documentation of changes to firewall rulesets. In addition, during the Compliance Audit, ReliabilityFirst discovered several other instances of failure to establish change control or configuration management. Specifically, URE failed to: a) establish configuration management for its generation business unit; and b) provide evidence of a change control or configuration management program for its information technology services business unit. In both cases, URE stated that it had processes in place, but URE did not provide adequate evidence of processes that would apply to devices randomly selected for the Compliance Audit.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to manage firewalls, a key primary defense for critical systems and operations, increased the risk of malicious activity that could compromise the BPS. In addition, URE's widespread failure to implement change control and configuration management significantly increased the likelihood of failing to restore CCAs in the event of critical failure. Lastly, because the instances of violation were rooted in a lack of configuration management processes, the violations were likely to recur until mitigated.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011103-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. change its change control and configuration management process to include documentation of firewall rule changes;
2. implement a configuration management system and a configuration management database; and
3. create a process to show the addition of systems within the configuration management database, including initial baselines.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014251 and RFC2014014252 CIP-004-3 R2 and R2.1 - OVERVIEW

RFC2014014251

ReliabilityFirst determined that URE did not review its cyber security training program for two consecutive years. In addition, some training material, specifically a web-based training course, was used for training but was not described in URE's cyber security training program.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk posed by the violation was that URE would inconsistently implement its training program as a result of not reviewing the program and not having all materials used for training actually documented in the training program. A lack of training or inconsistent training was determined to be the root cause of multiple violations resolved through the Settlement Agreement. This risk was only partially mitigated because URE had formal training material and a training program.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE's Mitigation Activities required URE to implement a new cyber security training program.

ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014252

ReliabilityFirst determined that URE did not provide evidence that contractors and service vendors were trained prior to being granted access to CCAs. In addition, URE failed to provide evidence that training was conducted at least annually. URE provided evidence forms that did not include training dates and evidence indicating that some personnel were granted access to CCAs prior to receiving training.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. During the Compliance Audit, URE had difficulty producing training data, indicating that this issue has a high likelihood of recurrence. In addition, there were multiple variations of issues with incomplete training documentation and failure to train during the required timeframes, indicating that URE had multiple process weaknesses in managing cyber security training records. These process

weaknesses could lead to a general lack of awareness of cyber security issues across the organization and its contracted staff. Additionally, insufficient training may degrade URE's ability to prevent and respond to cyber security incidents.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011538 to address the referenced violations. URE's Mitigation Plan required URE to address the root cause of the violation by identifying a single internal organization, the NERC Training Organization, to be responsible for all URE cyber security training and implementing a technology solution to enable non-badged vendors and contractors who previously fell into process gaps to complete cyber security training through a web-based delivery system.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014253 CIP-004-3 R3.3 - OVERVIEW

ReliabilityFirst determined that URE did not ensure that each Personnel Risk Assessment (PRA) included the date that the assessment was conducted, or that the PRA included a seven-year criminal check. This was consistent with all contractors and vendors ReliabilityFirst sampled during the Compliance Audit. URE obtained PRA data through a self-designed form provided to its vendors, but URE failed to collect sufficient information through its process to demonstrate compliance with CIP-004-3 R3.3. Additionally, ReliabilityFirst noted that the evidence provided was inconsistent and incomplete as a result of the siloed nature of the business units preparing the data and a lack of final review before submitting the evidence.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not ensuring that all contractors and vendors have PRAs potentially made URE susceptible to malicious acts by insiders, and the long duration of the violation increased this risk of harm. In addition, the root cause of the violation involved an ineffective process, which can lead to multiple instances of noncompliance. The risk was only partially mitigated because URE did have a process in place, although it was inadequate, and did require some evidence of background checks, although the evidence was insufficient.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011548 to address the referenced violations. URE's Mitigation Plan required URE to:

1. perform an internal audit to ensure its contractors and vendors had completed PRAs; and
2. update its process to ensure that, going forward, PRAs are completed consistently with NERC Standards, including an effort to ensure that attestations from contractors and vendors are accurate and to identify more effective methods of collecting PRA information from third parties.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2013013197, RFC2014013447, and RFC2014013997 CIP-004-3a R4.2 - OVERVIEW

RFC2013013197

ReliabilityFirst determined that URE did not maintain its list of personnel with authorized cyber or authorized unescorted physical access to CCAs when it failed to revoke access to CCAs for two individuals within seven calendar days of those individuals no longer requiring access to CCAs. In the first instance, URE did not revoke an employee's physical access to CCAs when the employee changed positions within URE and therefore no longer required access to CCAs. In the second instance, URE did not revoke an employee's physical access to CCAs when the employee's training qualifications lapsed, which URE identified as an instance of an employee no longer requiring access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an effective process. The risk was partially mitigated because, in both instances, URE had conducted PRAs on the employees and both PRAs were current and up-to-date. Additionally, both employees received proper training prior to being granted access to CCAs.

ReliabilityFirst determined the duration of the first instance to be from the date the first employee no longer required access to CCAs, through when URE revoked the employee's access. ReliabilityFirst determined the duration of the second instance to be from the date the second employee no longer required access to CCAs, through when URE revoked the employee's access.

URE submitted its Mitigation Activities within its Self-Reports. At the time of the violation, ReliabilityFirst believed this mitigation was sufficient because the root cause initially appeared to be an

isolated human error issue. However, URE later determined that the root cause was broader and related to ineffective processes, and thus URE later corrected this root cause through its subsequent Mitigation Plans under RFC2014013447 and RFC2014013997.

URE certified that it had completed its Mitigation Activities, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013447

ReliabilityFirst determined that during user access review, physical access for one retired employee had not been revoked within seven calendar days of the employee no longer requiring access to a CCA. URE revoked physical access for this retired employee upon discovery and verified that the retired employee did not have cyber access.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an ineffective process. The risk was partially mitigated because the employee was properly trained prior to gaining access, had a current PRA, and did not have any cyber access to any CCAs.

ReliabilityFirst determined the duration of the violation to be from the date URE should have revoked access to the CCA, through when URE revoked the access.

URE submitted its Mitigation Plan designated RFCMIT010551 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revoke physical access;
2. coach employees on proper revocation procedures;
3. review the efficacy of the revocation process; and
4. implement improvements identified from the process review, including implementation of a new tool to assist with revocation.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013997

ReliabilityFirst determined that in preparation for the Compliance Audit, URE completed a review of access records and discovered two instances in which physical access was not revoked within seven

calendar days. In one instance, URE was four days late in revoking access, and in the second instance, URE was 46 days late.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE failed to identify the violation outside the scope of an upcoming Audit, and URE demonstrated a lack of internal controls to quickly identify procedural failures. In addition, although the subjects of the Self-Report had only physical access to CCAs, not revoking access when it is no longer needed leads to increased risk of unwarranted access to those CCAs, and this type of violation was likely to recur as the root cause related to an ineffective process. The risk was partially mitigated because the individuals whose access had not been revoked had updated training and PRAs.

ReliabilityFirst determined the duration of the violation to be from the date URE was required to revoke access, through when URE revoked the access.

URE submitted its Mitigation Plan designated RFCMIT011102-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete a root cause analysis and document the process for provisioning and revoking access; and
2. create a process flow diagram, identify correct roles and responsibilities, and implement the process.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013623, RFC2014014015, RFC2014014207, and RFC2015015300 CIP-005-3a R1.5 and R1.6 - OVERVIEW

RFC2014013623

ReliabilityFirst determined that URE did not identify a certain class of routers and switches (Lightweight Directory Access Protocol, or LDAP) as being used in the access control and/or monitoring of the Electronic Security Perimeter (ESP) and therefore failed to afford the protective measures specified in CIP-005-3a R1.5.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. By not protecting the devices used for access control into the ESP, the ESP could be

compromised. Additionally, the violation occurred due to URE's misunderstanding of the applicability of the Standards and the duration was long before URE realized the error.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT010669 to address the referenced violations. URE's Mitigation Plan required URE to:

1. eliminate the LDAP system as the sole authentication system to gain access to routers and switches within the ESP; and
2. implement a new scheme that uses two-factor authentication to access a jump box, which serves as the sole access point into the ESP.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014015

ReliabilityFirst determined that URE identified its Security Information and Event Management (SIEM) system, which is located in its Corporate Data Center, as a Cyber Asset used in the access control and/or monitoring of an ESP, but failed to maintain a PSP around the Corporate Data Center.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to properly identify all protections necessary for a new Cyber Asset, the room that contained the SIEM system did have physical access protections such as continuous access control and monitoring through the use of card readers and security staffing. As a result, the Corporate Data Center had the same protective measures required by CIP-006-3c R3 despite the lack of a PSP designation.

ReliabilityFirst determined the duration of the violation to be from the date the URE installed the SIEM system that gave rise to the requirement to identify the Corporate Data Center as a PSP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011099 to address the referenced violations. URE's Mitigation Plan required URE to create a PSP around the Corporate Data Center, and the SIEM system and other newer Cyber Assets were validated as being within the boundaries of a PSP.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014207 and RFC2015015300

ReliabilityFirst determined that URE did not properly maintain documentation of CCAs and non-CCAs within ESPs. Specifically, ReliabilityFirst discovered two problems with drawings submitted by URE for the Compliance Audit. First, a CCA on the list of NERC CIP Cyber Assets was not found on the corresponding drawings. Second, two other CCAs on the NERC CIP Cyber Assets list did not appear on the drawings, but were found to have changed names. URE submitted to ReliabilityFirst a Mitigation Plan to address the Alleged Violation of CIP-005-3 R1.6 (RFC2014014207) and committed to complete the Mitigation Plan. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation for failure to mitigate (RFC2015015300) and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Although the violation was only a documentation issue, it was indicative of a larger procedural issue with a long duration and thus was likely to recur. Also, through ReliabilityFirst's Mitigation Plan verification efforts, ReliabilityFirst determined that URE inaccurately identified devices in its ESP and PSP drawings and therefore lacked a basic understanding of its ESPs, thus increasing the risk that URE's ESPs would not be effective and would allow for potential compromise of its CCAs.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011828 to address the referenced violations. URE's Mitigation Plan required URE to:

1. revise its existing list of CCAs to include related ESP and PSP designations; and
2. develop documents and implement a process to ensure that ESP, PSP, and asset type information is regularly validated and associated lists are updated to reflect the production environment.

RFC2014014410, RFC2015015143, RFC2014014011, and RFC2014014208 CIP-006-3c R1, R1.1 and R1.8 - OVERVIEW

RFC2014014410

ReliabilityFirst determined that an employee escorting a vendor into URE's System Operations Center left the vendor unescorted for a short period of time in order to place a phone call. The vendor was discovered by URE security and escorted by security for the remainder of his time onsite to complete maintenance work for which he was contracted.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had a visitor escort policy in place, and the violation appears to be an isolated human performance issue that was quickly identified and corrected by URE security.

ReliabilityFirst determined the duration of the violation to be the one day when URE failed to follow proper internal procedures while escorting a vendor.

URE submitted its Mitigation Plan designated RFCMIT011776-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. discipline the employee through the corporate positive discipline process; and
2. enhance its training program to include example violations relating to visitor escort procedures.

RFC2015015143

ReliabilityFirst determined that URE terminated an employee's physical access for failure to complete annual requalification training. However, the employee continued to work eight shifts in a power plant control room in a PSP despite not having physical access because other employees permitted him access. Later, the employee made multiple attempts to access the PSP by swiping his access card, which triggered an alarm in the plant security office. This alarm was the result of a newly developed control to alert security in case of three failed access attempts by the same person within an hour. A security officer investigated the alarm and found the employee in the control room. URE later learned that the employee's annual requalification training was almost past due and the access provisioner prematurely revoked access as a result of an error in the notification report identifying employees whose training was set to expire.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The risk that this specific employee would put the BPS at risk is low because the employee had a current PRA and no cyber access. Moreover, the employee's access to the PSP

was removed only as a result of failure to timely complete annual requalification training as opposed to a termination, which may increase the risk that the employee would use the access in such a way as to put the BPS at risk. However, the violation is indicative of a poor compliance culture as the employee continued to work eight shifts even though his access was removed and other employees allowed him access even though his access was removed. The cultural issue, if not fixed, could lead to other violations in the future.

ReliabilityFirst determined the duration of the violation to be from the first day the employee was permitted in the PSP despite having his access revoked, through the day the employee's access was reinstated as a result of completing his training.

URE submitted its Mitigation Plan designated RFCMIT011743-3 to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide the employee with training and URE reinstated the employee's access;
2. place a visual indicator inside all control rooms near the inside exit buttons to remind personnel opening the door to log and escort visitors;
3. conducted training for all CIP plant employees with respect to procedures for visitors;
4. modify the early notification report to the access provisioner to clearly distinguish between expired training and training that will expire; and
5. develop a process to proactively reassign work for individuals whose access will be revoked so that the individuals can work outside of the PSPs.

RFC2014014011

ReliabilityFirst determined that 13 separate openings in a six-wall border exceeded 96 square inches. Two openings of approximately 1,440 square inches each were discovered at one generating facility, a third opening of approximately 240 square inches was discovered at another generating facility, and the remaining ten openings of approximately 130 square inches were discovered at URE's a separate operations center. URE determined that the openings were a result of original construction conditions, with the exception of the 240 square inch opening, which was created during a repair of a water leak within the PSP at the facility.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Most of the 13 openings were sufficiently small and hidden so as to render penetration of the PSP unlikely. However, two of the openings were larger and allowed sufficient

space for penetration of the PSP. Additionally, the four-year duration of the violation indicates a general lack of rigor in URE's Compliance Program.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011101-1 to address the referenced violations. URE's Mitigation Plan required URE to remediate each of the openings, document a new process for performing work on PSPs to include contacting security to ensure compliance, and update the work management checklist used when work is completed on PSPs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014208

ReliabilityFirst determined that URE did not annually review certain documents used to support URE's physical security plan. Specifically, URE did not review 13 "as-built drawings," which URE identified as documents that detail the specifications of each PSP. During the audit, URE stated that the drawings are reviewed on an ad-hoc basis rather than annually.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Despite having a process in place that required review of the drawings, URE personnel failed to follow the policy, indicating a lack of focus on physical security, or compliance generally. Although the drawings were not reviewed annually as required by CIP-006 R1.8, URE attests that the drawings were reviewed during the duration of the violation.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011545 to address the referenced violations. URE's Mitigation Plan required URE to clarify the scope of the annual review of the physical security plan in its process documents and create a related review checklist for the annual review.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014209 and RFC2013013198 CIP-006-3a R5 and CIP-006-3c R5 - OVERVIEW

RFC2014014209

ReliabilityFirst determined that URE's physical security plan uses too narrow a definition of the term "unauthorized access attempts." During the Compliance Audit, URE subject matter experts explained that URE's determination that no unauthorized access attempts took place relied on URE's definition of an "unauthorized access attempt" as not including invalid attempts. URE defines "unauthorized access attempts" as either tailgating, access gained without authorization, or a visitor separated from an escort. These thresholds would not include failed attempts to access a secure area and therefore only would identify successful attempts at unauthorized entry, falling short of the requirement to monitor physical access to PSPs.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's definition of unauthorized access attempts include only successful security breaches and not attempts to access the PSP. Thus, URE's practice of relying on successful unauthorized access can lead to delayed detection and response to malicious activity.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011544 to address the referenced violations. URE's Mitigation Plan required URE to modify its relevant security procedure to instruct security officers to investigate cases of multiple failed access card-key reads at PSPs, in addition to the requirement of investigating cases of tampering and piggybacking.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2013013198

ReliabilityFirst determined that while performing a monthly physical barrier inspection of a PSP at a power plant, a security officer discovered that three PSP doors to a central control room had been tampered with, thus preventing the doors from latching securely. As a result, the security officer was able to open the doors without swiping an authorized access card-key. The security officer also determined that although a door-forced alarm should have sounded, it in fact did not operate. URE performed a root cause analysis and traced the cause of the alarm failure to a firmware upgrade. Although URE followed the established procedure for the upgrade, the vendor determined through this root cause analysis that an additional step was needed to clear device memory before conducting

the upgrade. URE also conducted an investigation with respect to the door tampering, but the investigation was inconclusive with respect to the reason for the tampering. As a result of this incident at the power plant, URE subsequently tested the alarm functionality of all PSP access points and discovered issues with two additional PSP access points at its System Operations Center, where the alarming system failed due to faulty wiring and hardware. URE also discovered issues with seven PSP access points at its Alternate System Operations Center and one access point at another power plant.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. The initiating action in this violation, an ongoing physical tampering of security systems, is a significant culture of compliance breakdown. In addition, although URE did eventually discover the issue through the implementation of internal detective controls, the condition was not discovered timely. Thus, the violation potentially put the BPS at serious risk for a long duration.

ReliabilityFirst determined the duration of the violation to be from the date the URE's firmware upgrade first affected its alarming capability, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT010465 to address the referenced violations. URE's Mitigation Plan required URE to:

1. initiate its alternate security measures, which include dispatching a security officer to perform a roaming security patrols around the PSP;
2. perform a root cause analysis, restore alarm functionality to the doors at the generation plant Control Room, replace the portion of hardware that malfunctioned, and redistribute the configuration data for the access points;
3. test the alarm functionality of these access points on a weekly basis for several months to ensure the alarms continued functioning properly;
4. test the alarm functionality of all 105 URE PSP access points and perform a network walk down which consisted of a visual inspection of all computer equipment in the relevant control room, validation of known computer equipment, and a search for any anomalies; and
5. provide refresher access training presentations to personnel at the power plant in question.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014211 CIP-007-3a R1.3 - OVERVIEW

ReliabilityFirst determined that URE did not provide evidence of testing for cyber security controls for one Cyber Asset. The device not tested was a virtual server located at a power plant. URE indicated that its vendor tests the device, but URE did not provide ReliabilityFirst with evidence of such a test.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. A failure to test security controls on new Cyber Assets and those with significant changes can result in the affected Cyber Assets failing to perform as expected. URE failed to detect a lack of security controls testing by its vendor, at least in part because URE failed to maintain policies or procedures that govern vendor testing. This lack of oversight led to a long running violation that is likely to recur in multiple ways due to a lack of process and procedure.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011541 to address the referenced violations. URE's Mitigation Plan required URE to assign an individual as a subject matter expert role for the group responsible for testing the Cyber Asset at issue, build an in-house test system, and update related documentation.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013998 CIP-007-1 R2 - OVERVIEW

ReliabilityFirst determined that URE did not ensure that only those ports and services required for normal and emergency operations were enabled. Specifically, URE lacked documentation identifying the ports and services required for normal and emergency operations for three Net Controllers managed by URE's information technology services organization (ITS), two operator interface server systems managed by URE's generation unit, and 18 paperless chart recorders within the generation unit.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Without proper documentation on ports and services, URE could not confirm whether it enabled only ports and services required for normal and emergency operations. Thus, URE could have had ports and services enabled that were not required for normal or emergency operation, which would have created vulnerabilities that expose the systems to a higher risk of compromise by potentially allowing more channels for undetected access into URE's critical systems. Given this risk, and the fact

that the violation would have continued except for preparation of evidence for the Compliance Audit, the risk to the BPS was serious and substantial.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011100-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. complete a baseline of ports and services for the operator interface server assets and Net Controllers and remove the paperless chart recorders from the ESP; and
2. revise the Technical Feasiblibility Exception (TFE) process to clarify expectations and allow subject matter experts to access existing TFEs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014013626, RFC2014014262 and RFC20141014114 CIP-007 R3, R3.1, R3.2 - OVERVIEW

RFC2014013626

ReliabilityFirst determined that URE did not assess patches for its routers and switches, of which there are approximately 50, within its ESP because URE did not interpret CIP-007-1 R3 to require assessments of firmware upgrades, which require the entire upgrade of the operating environment rather than the application of a single software patch targeted to solve a vulnerability. URE indicated that it conducted periodic, undocumented reviews of firmware releases.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011578-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. assess all networking devices for patch applicability;
2. perform industry survey to understand how other utilities manage security patching for these devices;

3. establish a process for assessing the firmware;
4. replace hardware and upgrade other devices where necessary; and
5. run monthly reports on network firmware that check for the current version of network firmware.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014114 and RFC2014014262

Regarding CIP-007-3a R3.2, URE did not document the implementation of applicable security patches for its server devices (which host URE's EMS applications), the date it last patched those devices as part of its mitigation for the same violation identified during its CIP Compliance Audit. In total, there were 75 security patches released for URE's EMS. URE indicated that a contributing cause for this violation was that it did not have a process map that clearly indicates the process for patch management.

Regarding CIP-007-3a R3.1, URE did not assess patches or security upgrades for its firewalls. In addition, when security patches were not applied, URE did not document compensating or mitigating measures. URE had interpreted that firewalls were not Electronic Access Control or Monitoring Systems (EACMS). Based upon this interpretation, URE protected these devices based on CIP-005 Requirements but did not follow the CIP-007 Requirements applicable to EACMS.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's EMS has a direct impact on the reliability of the BPS, and not patching it since its mitigation for its previous CIP audit (during which time 75 patches were released) left the system vulnerable and put the BPS at serious risk of exploitation. Additionally, firewalls are one of the primary security controls against realization of potential threats and compromise, and not patching them left the system vulnerable and put the BPS at serious risk of exploitation.

ReliabilityFirst determined the duration of the violation to be from the date URE last patched its EMS, through when URE completed its Mitigation Plan.

For RFC2014014114

URE submitted its Mitigation Plan designated RFCMIT011526 to address the referenced violation. URE's Mitigation Plan required URE to:

1. assess and install applicable patches and apply for TFEs where applicable and implement compensating measures;
2. increase staff assigned to patching processes and develop a process to ensure ongoing knowledge and staff availability for implementing patches; and
3. develop a comprehensive TFE process and improve its patch management process to clarify deadlines and actions required.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

For RFC2014014262

URE submitted its Mitigation Plan designated RFCMIT011537 to address the referenced violation. URE's Mitigation Plan required URE to:

1. assess all security updates for firewalls identified as cyber assets, and institute a process for periodic assessment updates and evidence submissions;
2. define a standard for EACMS that includes the firewalls at issue; and
3. update its work documents to provide common work instructions for managing patch management activities for firewalls.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014012 CIP-007-3a R4 - OVERVIEW

ReliabilityFirst determined that two SIEM devices, which are Cyber Assets used in the access control and/or monitoring of the ESP, are not technically capable of complying with CIP-007-3a R4 as they cannot implement antivirus software or other malicious software prevention tools. However, URE did not file a Technical Feasibility Exception (TFE) with ReliabilityFirst. URE has documentation from the vendor documenting the compensating measures applied to the SIEM devices to mitigate risk exposure.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation was a documentation issue as the SIEM device could not support antivirus or other malicious software prevention tools and the vendor has documented compensating

measures applied to the SIEM devices to mitigate risk exposure. Thus, there was no increased risk of harm to the BPS as a result of URE not applying for a TFE with ReliabilityFirst.

ReliabilityFirst determined the duration of the violation to be from the date URE deployed its SIEM system, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011105 to address the referenced violations. URE's Mitigation Plan required URE to amend an already approved TFE with ReliabilityFirst to include the documented compensating measures applied to mitigate risk exposure from the inception of the SIEM devices.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014215, RFC2014014216, and RFC2014014257 CIP-007-3a R5.1.2, R5.2, R5.2.3, R5.3, R5.3.1, R5.3.2, R5.3.3 - OVERVIEW

RFC2014014215

ReliabilityFirst determined that URE did not provide logs of user account activity for a minimum of 90 days. URE did not have logs for a certain device sampled by ReliabilityFirst during the Compliance Audit. The device stopped communicating with the SIEM system for 15 days. URE asserted that although the device was not communicating with the SIEM system, local logs could be provided from the device. However, ReliabilityFirst determined that the application logs did not provide sufficient evidence that logs of sufficient audit trails were created.

ReliabilityFirst determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Inadequate audit trails of user actions on CCAs can lead to missing cyber security events. However, the violation applied to only one device, and URE had logs, although the logs did not have sufficient detail.

ReliabilityFirst determined the duration of the violation to be the time during which URE could not provide logs of user account activity.

URE submitted its Mitigation Plan designated RFCMIT011534-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the job aid to clearly define steps that should be taken in the event of a logging failure detection;

2. change the process so that the alert goes directly to security, then to the specific business unit at issue; and
3. improve the agent-based logging failure detection trigger criteria to 24 hours.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014216

ReliabilityFirst determined that URE did not properly manage the scope and acceptable use of administrator, shared, and other generic account privileges, including factory default accounts. In addition, URE did not maintain an audit trail of the account use of administrator, shared, and other generic account privileges, including factory default accounts. More specifically, regarding CIP-007-3a R5.2, at one of URE's power stations, during the Compliance Audit, ReliabilityFirst found labels attached to a device monitor in the central control room that provided the shared account Username and Password required to gain initial access to the device after startup. URE conducted a thorough root cause analysis.

First, URE determined that a shared account was used when initiating the Remote Desktop Protocol sessions before the generation software was initiated because if individual accounts were used, it would require the operator to log out of the operating system session when control of the unit was to exchange hands, which in turn would terminate the generation application and create potential risk to the Critical Asset by terminating the operator's ability to maintain control of the Critical Asset. URE determined that the shared operating system account had limited privileges and the application deemed to be of highest risk in use under that shared operating system account had application level authentication implemented and authentication logged. Thus, URE believed that it could meet the requirement of tracking who had access to this shared account by using the generation application's user authentication logs.

Regarding CIP-007-3a R5.2.3, URE had a policy that requires an audit trail of accounts use. However, URE could not provide ReliabilityFirst with evidence of an audit trail for shared accounts. URE asserted that it did not interpret the requirement correctly and could not provide an audit trail of individual access to shared accounts. URE's interpretation was that it was required to log the "identity of which users can use the shared accounts," rather than to "identify users who did use the shared account" each time a shared account is used.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Regarding the shared username and password, inadequate shared account management can lead to inadvertent use of CCAs, which can result in compromise of CCAs. The risk posed by the discrete violation may have been partially reduced because of the limited privileges in the shared account and additional authentication required to access the critical software on the device. However, the overall risk posed by the violation is serious and substantial, because the contributing factors to the violation, the process gaps and lack of awareness as to CIP requirements by the individuals implementing the CIP Compliance Program, could have led to other violations. Regarding the individual audit trails, inadequate audit trails can lead to missing cyber security events, and URE did not track individual use at all.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011467-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. schedule quarterly clean desk walk downs at each plant to ensure no passwords or user identifications are posted;
2. validate the need for all current shared accounts;
3. implement a process for logging and review of logs for individual use of shared accounts and training on the process; and
4. install individual accounts and remove shared operator accounts for devices at issue.

RFC2014014257

ReliabilityFirst determined that URE did not meet the password requirements on all Cyber Assets and did not file a TFE where applicable. More specifically, first, for routers and switches, URE uses a jump box to reach the devices. Authentication occurs at the jump box, which uses corporate active directory. There is a built-in user identification that is used when the jump box is not available and the password parameters for this account are not set as per R5.3.1, R5.3.2, and R5.3.3. Second, for servers in URE's System Operations Center, those servers have shared accounts for which passwords were not changed in two consecutive years. Third, for Net Controllers used by the Physical Access Control Systems (PACS), it is not technically feasible to set password parameters on these devices. While URE has a TFE for password complexity, it did not submit a TFE for minimum characters of a password (R5.3.1) or annual password changes (R5.3.3).

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Use of built-in accounts along with weak passwords, and not timely changing passwords, increases the risk that malicious actors will discover passwords and compromise CCA information as it makes passwords easier to decipher and allows malicious actors more time to decipher passwords. Additionally, the root causes of the violations were systemic issues with processes surrounding passwords management and the TFE process and thus could result in additional violations.

ReliabilityFirst determined the duration of the violation to be from the last day of the previous Compliance Audit of URE for the CIP Reliability Standards, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011543 to address the referenced violations. URE's Mitigation Plan required URE to:

1. reset all server shared accounts;
2. compile a list of filed TFEs;
3. develop a process for creation, maintenance, and reference of TFEs;
4. establish an annual, manual password change process for shared accounts; and
5. develop a centralized account management process which includes comprehensive password management.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014238 CIP-007-3a R9 - OVERVIEW

ReliabilityFirst determined that URE did not review and update documentation specified in CIP-007-3a at least annually for seven of the sixteen documents sampled during the Compliance Audit. Specifically, URE did not conduct: 1) an annual review of information technology services organization NERC-CIP testing procedure; 2) a review of Preferred Provider Organizations (PPO) 291 testing procedures for CCAs; 3) an annual review of ITS-SCADA patch management susceptibility weight imaging (SWI); 4) an annual review of the NERC CIP requesting access to a critical and/or non-CCAs within the ESP document ; 5) an annual review of the PPO 289 managing and controlling CIP secured access document; 6) an annual review of the NERC-CIP shared access SWI document; and 7) an annual review of the NERC-CIP account password requirements SWI document.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. The root cause related to process gaps, indicating that the issues would have continued and additional reviews would have been missed. Not conducting annual reviews posed a risk that the procedures would not be updated as required, thus potentially leading to other violations.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011535 to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify a complete inventory of CIP-007 related documents and begin tracking all relevant documents in a compliance tracking tool that sends automatic notifications to document owners relating to reviews; and
2. develop a process to review and update documentation at least annually for the required documents.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014239 CIP-008-3 R1.6 - OVERVIEW

As evidence that URE tested its ITS Incident Response Plan, URE submitted documents relating to a paper drill exercise. However, ReliabilityFirst determined that URE was unable to establish how this exercise demonstrated testing of the ITS incident response plan. URE noted that there was not a one-to-one mapping of the exercise to the ITS incident response plan, but rather the subject matter experts were expected to know the plan and follow it during the exercise. Though the evidence reflected a paper drill exercise, it did not demonstrate sufficient and appropriate evidence for testing the ITS incident response plan. URE's ITS business unit did not have a standard that specified how the annual ITS incident response plan test shall be executed to ensure the exercise is compliant with the CIP-008 standard.

ReliabilityFirst determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE needs to completely test, and adjust as necessary, the ITS incident response plan to ensure the plan will be effective in an actual security incident. However, this risk was partially mitigated by the fact that URE's ITS incident response plan otherwise met the CIP-008-3 Requirements and URE attempted to perform an annual test of the incident response plan, thus reducing the risk that the plan would be ineffective in case of an actual security incident.

ReliabilityFirst determined the duration of the violation to be from the date by which URE was required to test its ITS incident response plan through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011519-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. develop a pre-specification defining the required level of evidence to comply with CIP-008;
2. develop the standard for proper execution of the incident response plan exercise;
3. update the incident response plan to remove inaccurate language indicating that certain actions were voluntary;
4. execute the updated required annual exercise; and
5. define an effective evidence test procedure to ensure the evidence collected during the annual exercise meeting the pre-specification.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014240 CIP-009-3 R1 - OVERVIEW

ReliabilityFirst determined that URE did not include all CCAs, such as storage area network (SAN) switches, within its ITS recovery plan. The switches were overlooked because the ITS recovery plan concentrated on only the application layer of the CCAs, and URE did not have a sufficient process for validating that the ITS recovery plan included all CCAs. Also, URE did not demonstrate evidence of an annual review of the ITS recovery plan.

ReliabilityFirst determined that this violation posed a serious or substantial risk to the reliability of the BPS. Not having sufficient information on CCAs in its ITS recovery plan could have prevented URE from restoring CCAs' functionality. Additionally, the lack of an annual review increased the risk that the ITS recovery plan would continue to be insufficient because URE would not have the opportunity to identify the deficiencies in order to correct them. SAN switches are critical pieces of equipment that are necessary to provide connectivity to SAN storage, which is used by the EMS. Lack of an adequate recovery plan or information related to these CCAs could cause significant delays in recovery of essential assets supporting the BPS.

ReliabilityFirst determined the duration of the violation to be from the date by which URE was required to conduct an annual review of the ITS recovery plan, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011542 to address the referenced violations. URE's Mitigation Plan required URE to update the ITS recovery plan to ensure it covers all CCAs and revise its asset validation process to reconcile and review the ITS recovery plan to ensure it covered all CCAs.

URE certified that it had completed its Mitigation Plan, and ReliabilityFirst verified that URE had completed all mitigation activities.

RFC2014014241 and RFC2015015301 CIP-009-3 R2 - OVERVIEW

ReliabilityFirst determined that URE did not provide sufficient evidence that it annually tested its recovery plans for its generation and ITS business units or its EMS. While URE submitted some evidence of URE's testing of the recovery plans, the evidence was insufficient. URE submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-009-3 R2 and committed to complete the Mitigation Plan by a certain date. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan on the assigned date. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation (RFC2015015301) for failure to mitigate and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. URE demonstrated a lack of understanding of what is required to exercise its recovery plans such that they could be relied on during an actual recovery situation. Thus, this, along with not having adequate documentation to cover all CCAs within the recovery plans, presented the risk that there could have been gaps in recovery capability, or delayed recovery during an actual event, which could have caused serious harm to the reliability of the BPS.

ReliabilityFirst determined the duration of the violation to be from the start date of the Compliance Audit period through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011829 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate-level recovery plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. have a defined standardized process for testing each of the recovery sub-plans;

3. include the process for testing a representative sample of information used to recover BPS cyber system functionality and the timeframe in which the test must occur; and
4. conduct recovery exercises for each of the recovery sub-plans.

RFC2014014013 and RFC2015015302 CIP-009-1 R4 and CIP-009-3 R4 - OVERVIEW

ReliabilityFirst determined that URE's ITS business units did not store on backup media information essential to successfully restore CCAs, including the EMS. URE's generation business unit did not store on backup media information essential to successfully restore CCAs, including eight operator control clients and four operator interface server assets. URE's EMS application continuity plan stated that the "active/active" site configuration and site switchover constitutes its ability to backup and restore. This configuration is commonly referred to as "N-1" (redundancy) and is not considered sufficient for back-up and restoration of CCAs.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. In order to accomplish the restoration of functionality of a CCA, URE needed to obtain the essential information to recover the asset and re-establish the functionality previously served by the failed asset. If URE would have lost a CCA, the information to recover the asset would not have been identified and available, hindering timely recovery of that CCA. The CCAs for which URE did not perform backup were essential to the reliable operation of the BPS and thus could have caused serious harm if not timely restored.

ReliabilityFirst determined the duration of the violation to be from the date by which URE committed to complete its initial Mitigation Plan, through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011830 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate level Recovery Plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. define standardized processes for testing each of the recovery sub-plans;
3. develop a specific recovery sub-plan that addresses specific recovery procedures and media testing procedures for new Version 5 generation systems and associated PACS and EACMS; and
4. conduct recovery exercises for the Recovery Sub-Plans.

RFC2014014242 and RFC2015015303 CIP-009-3 R5 - OVERVIEW

ReliabilityFirst determined that URE did not store on backup media information essential to successfully restore CCAs under CIP-009-1 R4; thus, it could not perform annual testing of that back-up media. URE submitted to ReliabilityFirst a Mitigation Plan to address the violation of CIP-009-3 R5 and committed to complete the Mitigation Plan by a certain date. However, despite ReliabilityFirst's onsite and offsite verification efforts, ReliabilityFirst could not reasonably verify that URE completed its Mitigation Plan on the determined date. Thus, ReliabilityFirst determined that the underlying violation was not sufficiently addressed and was ongoing. As a result, ReliabilityFirst found a new violation (RFC2015015303) for failure to mitigate and required URE to submit a new Mitigation Plan to address the underlying violation.

ReliabilityFirst determined that these violations posed a serious or substantial risk to the reliability of the BPS. In order to accomplish the restoration of functionality of a CCA, URE needed to obtain the essential information to recover the asset and re-establish the functionality previously served by the failed asset. If URE would have lost a CCA, the information to recover the asset would not have been identified and available as a result of no testing to ensure the backup media would be usable, hindering timely recovery of that CCA. The CCAs for which URE did not perform backup were essential to the reliable operation of the BPS and thus could have caused serious harm if not timely restored.

ReliabilityFirst determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its subsequent Mitigation Plan.

URE submitted its Mitigation Plan designated RFCMIT011827-1 to address the referenced violations. URE's Mitigation Plan required URE to:

1. create one corporate-level recovery plan for BPS cyber systems and subsequent standardized recovery "sub-plans" for each Cyber Asset type;
2. define standardized process for testing each of the recovery sub-plans;
3. develop a specific recovery sub-plan that addresses specific recovery procedures and media testing procedures for EMS and associated PACS and EACMS;
4. conduct recovery exercises for at least one asset;
5. type within each recovery sub-plans; and
6. exercise a media test procedure for at least one asset for each recovery sub-plan medium type.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one million seven hundred thousand dollars ($1,700,000) for the referenced violations. Additionally, ReliabilityFirst will perform a Spot Check of URE in 2016 to review URE's current state of compliance for a targeted sample of CIP Reliability Standard Requirements relating to some of the violations resolved in the Settlement Agreement that posed a serious and substantial risk to the reliability of the BPS.

In reaching this determination, ReliabilityFirst considered the following factors:

1. ReliabilityFirst considered 21 of the instant violations as repeat noncompliance with the subject NERC Reliability Standards for CIP-002 R3, CIP-004 R2, CIP-004 R3, CIP-004 R4, CIP-005 R1, CIP-006 R1, CIP-007 R1, CIP-007 R2, CIP-007 R3, CIP-007 R4, CIP-007 R5, and CIP-009 R1;
2. URE did not have a properly structured internal compliance program at the time of the violations, and ReliabilityFirst did not award any mitigating or above and beyond credit for improvements for the current commitments to improve its culture given the nature of the violations, the long duration of the violations, and URE's slow response to the violations;
3. ReliabilityFirst awarded mitigating credit for URE's implementation of an application to automate some steps for access revocation and provisioning;[2]
4. URE self-reported 17 violations (RFC2014014014, RFC2013013197, RFC2014013447, RFC2014013997, RFC2014013623, RFC2014014015, RFC2014014410, RFC2014014011, RFC2015015143, RFC2013013198, RFC2014013998, RFC2014013626, RFC2014014262, RFC2014014114, RFC2014014012, RFC2014014013, and RFC2015015302), although most of those Self-Reports were submitted to ReliabilityFirst leading up to and following the Compliance Audit. 19 violations were found during a Compliance Audit (RFC2014014245, RFC2014014251, RFC2014014252, RFC2014014253, RFC2014014207, RFC2015015300, RFC2014014208, RFC2014014209, RFC2014014211, RFC2014014215, RFC2014014216, RFC2014014257, RFC2014014238, RFC2014014239, RFC2014014240, RFC2014014241, RFC2015015301, RFC2014014242, and RFC2015015303);

[2] The application includes alerts and controls to help maintain compliance with respect to such things as provisioning the correct level of access, requiring training prior to provisioning access, and timely revoking access where required. Additionally, URE is in the process of implementing a tool to automate and track requests for password changes, logs access, and the usage of privileged accounts. These tools enhance security and reliability beyond that which is required by the CIP Reliability Standards.

5. URE received some mitigating credit for URE's submission of some Self-Reports that were submitted well in advance of the Compliance Audit;
6. URE was not cooperative throughout the compliance enforcement process, and ReliabilityFirst considered URE's lack of cooperation as an aggravating factor in the penalty determination;[3]
7. the violations of RFC2014014015, RFC2014014410, RFC2014014012, and RFC2014014215 posed a minimal and not a serious or substantial risk to the reliability of the BPS. The violations of RFC2014014245, RFC2014014253, RFC2013013197, RFC2014013447, RFC2014013997, RFC2014014011, RFC2014014208, RFC2015015143, RFC2014014238, and RFC2014014239 posed a moderate and not a serious or substantial risk to the reliability of the BPS. The violations of RFC2014014014, RFC2014014251, RFC2014014252, RFC2014013623, RFC2014014207, RFC2015015300, RFC2014014209, RFC2013013198, RFC2014014211, RFC2014013998, RFC2014013626, RFC2014014262, RFC2014014114, RFC2014014216, RFC2014014257, RFC2014014240, RFC2014014241, RFC2014014241, RFC2014014013, RFC2015015302, RFC2014014242, and RFC2015015303 posed a serious risk to the reliability of the BPS; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one million seven hundred thousand dollars ($1,700,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[3] Following the Compliance Audit, ReliabilityFirst experienced difficulty in obtaining substantive updates from URE regarding its mitigation progress. Despite numerous requests for updates following the Compliance Audit, ReliabilityFirst did not receive the majority of Mitigation Plans or substantive updates on mitigation progress until later than requested. URE also had more recent issues with delays in submitting and completing Mitigation Plans.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 9, 2016 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one million seven hundred thousand dollars ($1,700,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Robert K. Wargo* Vice President Reliability Assurance & Monitoring ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0682 Phone 216-503-9207 Facsimile bob.wargo@rfirst.org Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0683 Phone 216-503-9207 Facsimile jason.blake@rfirst.org Deandra Williams-Lewis* Director of Enforcement ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0689 Phone 216-503-9207 Facsimile deandra.williamslewis@rfirst.org	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Kristen M. Senk* Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 216-503-0669 Phone 216-503-9207 Facsimile kristen.senk@rfirst.org	Gizelle Wray* Associate Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3016 (202) 644-8099 – facsimile gizelle.wray@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net
(202) 400-3000
(202) 644-8099 – facsimile

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

April 28, 2016

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP16-__-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

NERC respectfully requests that the Commission accept this Spreadsheet NOP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
2	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013763	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-003-3 R5. ReliabilityFirst_URE1's documented program for managing access to protected Critical Cyber Asset (CCA) information does not clearly define a process for maintaining a list of designated personnel responsible for authorizing access to protected CCA information and validating that list on an annual basis. Specifically, ReliabilityFirst_URE1 failed to properly and timely document the addition and removal of authorizers to protected CCA information. ReliabilityFirst_URE1 was keeping two lists for documenting its authorized access approvers to protected CCA information. The first list was maintained manually in an Excel spreadsheet and is known as the Information Protection Owner List. The second list, known as the Number 1 and 2 Report, was an automated system-based list that is generated from ReliabilityFirst_URE1's Active Directory. The Number 1 and 2 Report was used to annually review the processes for controlling access privileges to protected information. When compared, ten differences in documented authorizers were identified between the two lists. ReliabilityFirst_URE1 also lacked adequate evidence to establish that it fully performed an annual review of the list of authorized approvers. The root cause of this violation relates to the management practice of verification, ReliabilityFirst_URE1 did not have a procedure to ensure accuracy between the lists after modifications The differences in documented authorizers between the two lists arose from uncorrected human performance errors in manually updating the lists. The errors, such as former approvers being removed from one list and remaining on the other list, were not caught or corrected because ReliabilityFirst_URE1 did not have a process step built into its procedure to compare both lists to ensure accuracy after a change was made to one or both lists. This lack of built-in verification allowed the errors in each list to go uncorrected.	CIP-003-3	R5	Lower	Severe
3	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014014186	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-004-3a R4. ReliabilityFirst_URE1 identified that lists of personnel with authorized cyber or authorized unescorted physical access have not been maintained in accordance with CIP-004 R4. All relevant access control information was retained across various systems, but ReliabilityFirst_URE1 determined that the collective set of information was not maintained and consolidated in a manner to facilitate prompt and accurate reviews. ReliabilityFirst_URE1 also identified instances where lists were not updated and accesses were not revoked within the seven-day timeframe required under CIP-004 R4.1 and CIP-004 R4.2. ReliabilityFirst_URE1 conducted a review of all quarterly certifications of logical and physical access conducted during prior years. Through this review, ReliabilityFirst_URE1 identified and confirmed a total of 66 accounts where access was not revoked within the seven day timeframe under CIP-004 R4. These instances were the result of gaps in ReliabilityFirst_URE1's access revocation procedures. ReliabilityFirst_URE1 discovered that the identification of new access control lists for CIP resources that are in-scope is not a documented process and relies primarily on manual investigation. Similarly, the consolidation of the in-scope access control lists into one authoritative list of all personnel with CIP information, electronic, and physical access is not a documented process. Monitoring of active access revocation requests and of accounts with pending training expiration is not sufficiently documented and relies primarily on manual investigation. Escalation of access revocation requests nearing completion deadlines and identification of all access rights held by a CIP access holder that are to be revoked are both insufficiently documented and rely primarily on manual investigation. Certain technical limitations at ReliabilityFirst_URE1 resulted in an over-reliance on manual investigations and processes in lieu of automated processes. The root cause of this violation related to the management practice of verification. ReliabilityFirst_URE1 relied on manual processes for creating, managing, and reviewing its lists of personnel with CIP access and for responding to access revocation requests. ReliabilityFirst_URE1's	CIP-004-3a	R4	Lower	Higher

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
2	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. ReliabilityFirst_URE1 uses formal self-assessment processes to assess compliance to the Standard, which are separate from maintaining the list of authorizers and verifying the list of authorizers during the annual review. For restricted information, all repositories are housed on ReliabilityFirst_URE1 internal networks and to access any repository, an individual must be on the ReliabilityFirst_URE1 system and have ReliabilityFirst_URE1 assigned credentials. Most restricted information is housed on shared drives and similar repositories that have department and or team level access restrictions, which require specific approvals by a manager or higher. ReliabilityFirst_URE1's access request system routes any access requests to the current owner of a protected information repository. The repository owner typically has the best direct knowledge of the need for that access and is in the best position to assess whether that access should be granted. This setup mitigates the risk posed by this violation because the current authorized approvers are still in control of approving and rejecting access to protected information repositories.	when ReliabilityFirst_URE1 was required to comply with the Standard	when ReliabilityFirst_URE1 created a single, accurate list of authorized access approvers to protected CCA information
3	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Physical access badges, laptops, and network IDs are all revoked and disabled immediately upon an individual's termination or departure, which minimizes the risk of unauthorized access once an employee or contractor has left the company because the individual can no longer access any Physical Security Perimeters or Electronic Security Perimeters. Additionally, none of these individuals were terminated for cause. Each of the 66 individuals that did not have their access revoked within the seven-day timeframe was a trusted employee or contractor with a valid Personnel Risk Assessment and CIP training. Lastly, for all of the identified instances where access lists were not updated or access was not revoked in a timely fashion, there were no occurrences where such accesses were exploited or misused.	when ReliabilityFirst_URE1 failed to revoke user access	when ReliabilityFirst_URE1 revised its access revocation procedure to ensure timely processing of CIP access removals and revocations

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) resolved identified discrepancies between existing authorized approver lists to create a single accurate list of authorized approvers; 2) assessed existing procedures and the current plan for integration with the legacy program and developed a plan to either revise these procedures or accelerate integration; 3) developed a detailed plan and schedule for the implementation of revised procedures and integration; 4) developed and delivered training to all impacted personnel responsible for maintaining and annually verifying the authorized approver list; 5) implemented the improved and integrated program for the maintenance and annual verification of the authorized approver list; and 6) performed a quality assurance assessment to verify that the improved and integrated program is operating as intended and will remediate any discrepancies. ReliabilityFirst_URE1 also assessed opportunities for further process improvements and developed a report on conclusions from the assessment. After this assessment, ReliabilityFirst_URE1 determined that two enhancements and communications can be mad to further the annual review process. 1) Revise the ReliabilityFirst_URE1 CCA Information Protection Procedure. 2) Revise the Access and Account Monitoring Procedure. ReliabilityFirst_URE1 confirmed in its evidence that it completed these two revisions.	1/30/2015	9/11/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.
3	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) verified that the current authoritative list of in-scope CIP resources is comprehensive; 2) developed a process for determining, managing, and reviewing that all in-scope access control lists are documented and accounted for; 3) developed a method to clearly view and prioritize all open CIP access revocation tickets based on the required due date to revoke access; 4) revised the Access Revocation Procedure to ensure timely processing of CIP access removals and revocations; 5) developed a checklist/job aid to accompany the revised Access Revocation Procedure; 6) reviewed and revised the Access and Account Monitoring Procedure; 7) provided training on the revised Access Revocation Procedure to responsible personnel; 8) developed a process and associated documentation for creating a single consolidated list of personnel with CIP information, electronic, and physical access; 9) performed a quality assurance assessment to verify that the improved and revised process is operating as intended; 10) provided training and communications on the above access control lists maintenance process and procedure changes to responsible personnel; and 11) performed an overall quality assurance assessment to verify that all process enhancements for both CIP access removals and CIP access list maintenance are being executed in accordance with revised procedures. A part of the entity's CIP Version 5 implementation program includes an access controls and automation project, which includes an identity and access management solution called the Access Controls and Automation System (ACAS). The ACAS will centralize access management and governance processes and procedures and support CIP Version 5 compliance. The improved automation in ACAS will provide benefits to ReliabilityFirst_URE1 and assist in preventing similar access issues from reoccurring in the	6/15/2015	10/26/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-004 R4 compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
4	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013840	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-1 R1. ReliabilityFirst_URE1 stated that during an internal review of its Cyber Vulnerability Assessment (CVA) findings, ReliabilityFirst_URE1 identified that it did not have adequate evidence of the assessment of the following two types of Electronic Access Control and Monitoring Assets (EACMs) pursuant to CIP-005 R1.5: Security Event Monitoring System and Intrusion Detection System. While ReliabilityFirst_URE1 collected and analyzed data for 10 Security Event Monitoring an Intrusion Detection assets as part of the CVA assessment, the CVA report did not clearly state that the assets did not have any identified vulnerabilities. ReliabilityFirst_URE1 had a lack of clear evidence linking the various phases, from raw data to the analysis, the assessment, and the final report of the CVA process. As part of an extent of condition review, ReliabilityFirst_URE1 identified that eight assets were not configured to forward their internal asset logs to a log repository, which comprises this violation of CIP-005-1 R1. The root cause of this violation related to the management practice of asset and configuration management. ReliabilityFirst_URE1 maintained weak procedural controls for the generation and documentation of the CVA analysis and report, particularly in managing contractor performance in support of compliance activities. As a result of these weak procedural controls, the assets were not adequately inventoried and monitored in the CVA assessment and report.	CIP-005-1	R1	Medium	Severe
5	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014014535	Settlement Agreement	ReliabilityFirst determined that ReliabilityFirst_URE1 was in violation of CIP-005-1 R1 as a result of a Compliance Audit. ReliabilityFirst_URE1 had not identified all access points to the electronic security perimeters (ESPs). ReliabilityFirst_URE1's vendor identified and recommended that ten assets, which are Critical Cyber Assets (CCAs), that had not previously been declared as ESP access points should be declared as ESP access points. ReliabilityFirst_URE1 updated its documentation to correctly identify these ten assets as ESP access points. ReliabilityFirst_URE1 was also able to show that all ten of the newly identified assets were being provided all security controls as required by CIP-002 through CIP-009. The root cause of this violation related to the management practice of workforce management. ReliabilityFirst_URE1 employees did not fully understand the CIP-005-1 R1 requirements, as ReliabilityFirst_URE1's subject matter experts focused only on routable traffic crossing the ESP in defining electronic access points. ReliabilityFirst_URE1 did not understand that non-routable data traffic crossing an ESP boundary needed to have a defined electronic access point.	CIP-005-1	R1	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
4	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All the assets in question were external to the ReliabilityFirst_URE1-defined NERC CIP Electronic Security Perimeters (ESPs) and had very limited communication ability with specific assets within the ESPs. The assets that did not log had a minimal impact to the Bulk Electric System because they had no direct control function or telemetry monitoring of critical assets. ReliabilityFirst_URE1 also employs a layered security model. These assets have been deployed within their own regulated private network, which is separate from both the business and control networks, and the hosts themselves have been hardened – all mitigating the risk posed by the violation. Lastly, at the time of the assessment, the assets were meeting all of ReliabilityFirst_URE1's security controls.	when ReliabilityFirst_URE1 was required to comply with the Standard	when the assets were fully incorporated into ReliabilityFirst_URE1's CVA
5	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All the assets in question were external to the ReliabilityFirst_URE1 defined NERC CIP Electronic Security Perimeters and had very limited communication ability with specific assets within the ESPs. The assets that did not log had a minimal impact to the Bulk Electric System (BES) because they had no direct control function or telemetry monitoring of critical assets. ReliabilityFirst_URE1 also employs a layered security model and these assets have been deployed within their own regulated private network which is separate from both the business and control networks and the hosts themselves have been hardened – all mitigating the risk posed by the violation. Lastly, at the time of the assessment, the assets were meeting all of ReliabilityFirst_URE1's security controls.	when ReliabilityFirst_URE1 was required to comply with the Standard	when ReliabilityFirst_URE1 updated its documentation - ESP Diagram - to correctly identify the CCAs in question as ESP access points

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
4	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) reviewed the existing processes for maintaining CVA evidence, particularly with regard to EACMS; 2) communicated requirements for documenting and retaining CVA evidence to all responsible and impacted personnel; 3) conducted the incomplete CVA, including all EACMs devices; and 4) performed a quality assurance assessment to confirm that evidence of performing the CVA for EACMS was appropriately documented and maintained in accordance with established processes.	1/30/2015	8/17/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-005 R1 compliance history to be an aggravating factor in the penalty determination.
5	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Compliance Audit	To mitigate this violation, ReliabilityFirst_URE1: 1) reviewed the existing processes for maintaining CVA evidence, particularly with regard to EACMS; 2) communicated requirements for documenting and retaining CVA evidence to all responsible and impacted personnel; 3) conducted the CVA, including all EACMS devices; and 4) performed a quality assurance assessment to confirm that evidence of performing the CVA for EACMS was appropriately documented and maintained in accordance with established processes.	1/30/2015	8/17/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-005 R1 compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
6	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013760	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-3a R3. ReliabilityFirst_URE1 identified a set of Critical Cyber Assets (CCAs) that were not properly configured to log at the time of installation. ReliabilityFirst_URE1 implemented the Security Event Monitoring system. This system is used to meet the technical requirements for logging, monitoring, and alerting under CIP-005 R3, CIP-007 R5.2.3 and CIP-007 R6.5. The security event monitoring system has been used to collect asset logs, alert on specific event criteria, and provide reports for event monitoring since its installation. ReliabilityFirst_URE1 identified that when the syster was installed, eight hardened assets were not configured to forward their internal asset logs to the log repository. In addition, an intrusion detection system was also installed the same year. This system is used to meet the requirements for detecting actual unauthorized access under CIP-005 R3.2. The intrusion detection system has been used to investigate anomalous network traffic since installation. ReliabilityFirst_URE1 identified that the method the intrusion detection system uses to alert does not meet the CIP-005 R3.2 requirement. It identifies suspicious or anomalous network traffic and alerts these events to its internal dashboard. It is not capable of alerting externally, meaning it only presents the alert on the internal console dashboard. Upon realization that CIP-005 R3 requires external automated alerting, ReliabilityFirst_URE1 should have requested a Technical Feasibility Exception (TFE) because the intrusion detection system only provides manual alerting. ReliabilityFirst_URE1 failed to submit a TFE request. The root cause of this violation related to the management practice of workforce management. Specifically, the root cause was a misunderstanding of the requirements of CIP-005 R3. ReliabilityFirst_URE1 incorrectly believed that manual monitoring, without an approved TFE, was acceptable under CIP-005 R3. ReliabilityFirst_URE1's misunderstanding meant it did not request TFEs or implement an automated system that would have achieved compliance.	CIP-005-3a	R3	Medium	Severe
7	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013839	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-005-3a R5. During review of evidence as part of an extent-of-condition analysis, ReliabilityFirst_URE1 identified instances where it did not have sufficient evidence to establish the timely completion of annual reviews and approvals of documentation specified in CIP-005-3 R5 that is subject to annual review obligations. Specifically, ReliabilityFirst_URE1 identified 26 procedures that are subject to the CIP-005 R5 annual review requirement. ReliabilityFirst_URE1's program defines annually as once per calendar year and no more than 16 months between events or activities. For two of those 26 procedures, CIP Security Alert and System Monitoring Procedure and CIP Access Authorization Procedure, ReliabilityFirst_URE1 did not have clear evidence in the revision history of each document showing tha an annual review and approval meeting the ReliabilityFirst_URE1 annual criteria was performed. The root cause of this violation related to the management practices of verification and asset and configuration management. There was no built-in check to verify that all procedures and documents that were to be updated had clear evidence in their revision history to indicate that an annual review and approval had been performed. Additionally, the procedures and associated documents did not have a clear owner, an individual responsible to make sure that the update was properly completed. This lack of a clear owner meant the procedures were not effectively inventoried or monitored.	CIP-005-3a	R5	Lower	Moderate

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
6	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The security event monitoring assets that did not log had no direct control function or telemetry monitoring of critical assets. Although a compromise of the assets would place the logging of the specific CIP assets at risk, the monitoring and alerting of the other CIP assets would generally identify anomalous behavior. This monitoring and alerting minimize the risk that an actual impact to a CIP asset could occur without being detected. Unauthorized access to the assets would not allow any access to any other NERC Cyber Asset, CCA, Electronic Access Control and Monitoring Assets (EACMs), or Protected Cyber Assets (PCAs). For the intrusion detection system violation, system events and signature alerts are reviewed on a regular basis, thereby minimizing any risk as a result of the system's inabili to alert in accordance with the requirements of CIP-005 R3. During those reviews, no unauthorized access events or any malicious events were detected. All of the actions required to meet the standard commitments were put in place when the intrusion detection system was installed. This is a primarily documentation violation as it arose from not completing a TFE.	when ReliabilityFirst_URE1 installed the security event monitoring system	when ReliabilityFirst_URE1 properly configured all of its security event monitoring assets to forward their internal asset logs to the log repository and filed a TFE
7	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The missed annual reviews pose minimal risk because all lists and diagrams that relate to CIP operational concerns were reviewed and approved annually so there were no potential security or protection impacts related to missed annual reviews. ReliabilityFirst_URE1 assesses compliance through formal self-assessment processes and not by the installation of updates. Updates are completed to meet the specific CIP obligation that requires the update and to identify areas of improvement. Additionally, all updates were completed, though not always on time or with complete documentation.	when ReliabilityFirst_URE1 failed to show it performed an annual review	when ReliabilityFirst_URE1 obtained evidence showing that the two procedures had a completed annual review and approval that met ReliabilityFirst_URE1's internal criteria

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
6	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) implemented measures to ensure the identified security event monitoring assets are forwarding their logs; 2) conducted an assessment of existing processes and defined interim improvements to ensure that new EACMS devices are properly configured to log at the time of installation; 3) developed and delivered training to impacted personnel responsible for implementing process improvements and controls; 4) prepared and filed a TFE for the intrusion detection system alerting instances where the CIP-005 R3 requirement cannot be met; 5) developed a plan to transition to a significant change testing program; 6) conducted training on the change testing program; 7) communicated the implementation start date of change testing procedure to all impacted personnel; and 8) performed a quality assurance assessment on a sample set of newly installed devices to verify that the significant change testing procedure is being implemented as intended.	6/29/2015	10/26/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.
7	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) developed an inventory of all CIP-005 documentation that is subject to the annual review requirement in preparation for the previous year's annual reviews; 2) reviewed the inventory to assess annual review completion dates and to determine which documents, if any, were not reviewed within the 2013 annual review timeframe; and 3) conducted and completed annual reviews of all ReliabilityFirst_URE1 CIP-005 documents in inventory as part of the company-wide annual review process, ensuring that any documents identified as part of the inventory review are reviewed and approved within the annual review timeframe.	12/31/2014	4/8/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
8	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014014167	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-3c R1. A ReliabilityFirst_URE1 intern working as an escorted visitor, and the intern's escort breached the applicable ReliabilityFirst_URE1 CIP visitor access program within a Physical Security Perimeter (PSP). While the ReliabilityFirst_URE1 intern's Personnel Risk Assessment (PRA) and CIP training were complete, his unescorted access approval was not yet approved. Therefore, the ReliabilityFirst_URE1 intern was still being treated as a visitor. During the visit, the ReliabilityFirst_URE1 intern was left alone within the PSP for approximately 22 minutes, while the escort met with other personnel down the hall. During this time, the intern attempted to badge out of the PSP to use the restroom. Due to the established access controls, his exit was denied and a door alarm notification was transmitted to the Security Operations Center (SOC). Immediately upon receipt of the door alarm notification, the SOC reported the incident to the security guard on duty, who responded, spoke with the intern and his escort, and verified the source of the alarm. ReliabilityFirst_URE1 failed to maintain continuous escorted access of a visitor within the PSP. The root cause of this violation related to the management practice of workforce management through a lack of effective training. The ReliabilityFirst_URE1 employee escorting the intern within the PSP did not follow ReliabilityFirst_URE1 procedures and protocols for escorting a visitor within a PSP by leaving the intern unattended in a PSP.	CIP-006-3c	R1; R1.6	Medium	High
9	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013759	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-006-1 R2. ReliabilityFirst_URE1 determined that certain Physical Access Control Systems (PACS) devices associated with the building control system (BCS) were not afforded all of the protective measures and controls required under CIP-006 R2.2. Two sets of BCS assets were affected. The first set of assets, BCS servers and workstations, had been appropriately classified as PACS, however, ReliabilityFirst_URE1 had insufficient evidence to demonstrate that the PACS had been afforded all of the protective measures and controls required under CIP-006 R2.2. In this first set of assets, a total of two BCS servers and six BCS workstations were affected. The second set of assets involved BCS net controllers that had not been appropriately classified as PACS. As a result, the BCS net controllers were not afforded any of the protective measures and controls required under CIP-006 R2.2. A total of three BCS net controllers were impacted. ReliabilityFirst_URE1 is currently in the process of retiring the BCS System and transitioning its PACS to a different system. The root cause of this violation related to the management practices of workforce management through a lack of effective training and ineffective asset and configuration management. ReliabilityFirst_URE1 did not adequately train the new BCS application support team, as the team did not properly identify the appropriate BCS assets as PACS and did not complete all documentation requirements. The BCS assets were also not properly inventoried or monitored, as some BCS net controllers were not classified as PACS.	CIP-006-1	R2; R2.2	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
8	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. ReliabilityFirst_URE1 has live video surveillance cameras positioned to view both the interior and exterior sides of the EOB PCS Room PSP access point. The Security Operations Center (SOC) has the ability to view live and recorded video for these cameras. This video can also be viewed from the guard station at the electric operations building at ReliabilityFirst_URE1. In addition to the video surveillance, on site security staff performs a minimum of two walk-through security checks of the PSP per 8-hour shift. The PSP included a limited number of Critical Cyber Assets (CCA) in the PSP associated with ReliabilityFirst_URE1's Energy Control System (ECS). There were no other assets requiring CIP protection such as EACMS, EAP, or PACS in the PSP. These CCA require a user ID and password to be entered to log onto the computer, and a separate user ID and password to be entered in order to access the ECS application. In addition to the CCAs, there are desktop computers in the PSP connected to the corporate data network, but any attempt to access assets subject to CIP protection require a separate user ID and password for remote access via a jump server, as well as two-factor authentication, none of which was available to the intern. All wall and desk cabinets within the PCS Room that contain any CIP information are locked. The ReliabilityFirst_URE1 intern involved had already completed his PRA and CIP training and was being escorted as a visitor while the approval of his physical unescorted access request to the PSP was being completed, and was left unescorted for a short period of time. Additionally, on attempting to exit, the security alarms were triggered to notify the SOC, who reported the incident to the security guard on duty, who responded and verified the source of the alarm. ReliabilityFirst_URE1 promptly identified, responded to, and corrected the Alleged Violation. All security controls worked as designed when the ReliabilityFirst_URE1 intern attempted to exit the PSP without proper authorization or an escort.	when the intern was left unescorted within the PSP	when ReliabilityFirst_URE1 conducted a mandatory stand-down meeting with all relevant personnel to reinforce visitor access processes
9	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The identified PACS cyber assets do not support critical functions and operations for the Bulk Electric System. Additionally, all assets affected currently reside within a defined Physical Security Perimeter (PSP). In order to physically access those devices, an individual would need authorized unescorted physical access to the PSP in which they reside. ReliabilityFirst_URE1 also did not identify any instances of deliberate attempts to circumvent existing physical access controls. The assets in question are afforded a baseline level of protection based on ReliabilityFirst_URE1's general corporate policies and procedures and a defense-in-depth security strategy.	when ReliabilityFirst_URE1 was required to comply with the Standard	when ReliabilityFirst_URE1 installed CIP controls for the new system and effectively retired the BCS System

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
8	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1 conducted a mandatory stand-down meeting, with all relevant personnel. During this meeting, the PSP visitor access processes were reviewed and reinforced to ensure that all personnel adequately understood the importance of following all aspects of ReliabilityFirst_URE1 visitor access processes and procedures at all times. The discussion included a particular emphasis on personnel responsibilities when escorting individuals in protected areas, and the importance of physical security and compliance with the NERC CIP Standards. To prevent recurrence, ReliabilityFirst_URE1 also: 1) developed a checklist to support PSP visitor access program which details the requirements and responsibilities of personnel escorting a visitor into a PSP; 2) updated applicable ReliabilityFirst_URE1 visitor access procedures to include the new checklist and required that the checklist be distributed to and reviewed with escorting personnel at the time a visitor is being processed and before the escort begins; 3) trained security performing personnel on the new checklist requirement; and 4) communicated the new checklist requirement to all personnel with authorized unescorted PSP access.	12/19/2014	1/27/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-006 R1 compliance history to be an aggravating factor in the penalty determination.
9	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) developed a comprehensive plan to retire the BCS System and transfer to the new system. This transfer included technical and procedural controls and the identification of any Technical Feasibility Exceptions (TFEs) as necessary; 2) performed the cutover to the new system and applied CIP controls; 3) trained impacted personnel who will be responsible for performing compliance activities on all requisite CIP controls being applied to the new servers, workstations, and net controllers; and 4) performed a quality assurance assessment to verify that the implemented controls are operating as intended and assessed opportunities for improvement.	7/31/2015	10/26/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
10	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013758	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R1. ReliabilityFirst_URE1 discovered it had insufficient evidence of cyber security controls testing associated with certain cyber assets as required under CIP-007 R1. Specifically, ReliabilityFirst_URE1 identified an instance where security control testing was not fully documented for one redundant Electronic Access Control and Monitoring Asset (EACMS) syslog server. After this initial identification, ReliabilityFirst_URE1 further identified eight EACMS logging devices where cyber security controls testing evidence and results were not fully retained and documented as required by ReliabilityFirst_URE1 procedures. Additionally, ReliabilityFirst_URE1 found similar documentation issues with 11 Physical Access Control Systems constituting BCS Servers, workstations, and net controllers. ReliabilityFirst_URE1 failed to document and retain cyber security controls testing evidence. The root cause of this violation related to the management practice of workforce management through ineffective training. Personnel responsible for installing or performing significant changes for cyber assets were confused about their responsibilities, particularly whose responsibility it was to document pre-change conditions. This confusion occurred due to the insufficient training given to the responsible personnel on the cyber security controls testing process and documentation requirements.	CIP-007-3a	R1	Medium	Severe
11	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014014094	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-1 R3. ReliabilityFirst_URE1 failed to properly monitor four firewalls and failed to properly inventory and document 13 patches for ten switches. ReliabilityFirst_URE1 recently began to implement patch management tools to provide a greater degree of automation. These enhanced compliance tools allow ReliabilityFirst_URE1 to generate reports for all issued patches for a certain period of time in order to effectively and timely assess each patch for possible implementation. After these improvements were implemented, an initial report was run to verify patching assessments. This report revealed that some CIP-007 R3 patching controls were not applied in accordance with ReliabilityFirst_URE1 processes for a set of CIP-classified assets and intrusion detection system (IDS) assets. For four firewalls, ReliabilityFirst_URE1 identified one patch that was assessed but not implemented, two patches that were mistakenly assessed as not applicable, and three assessed patches were not required to be assessed by ReliabilityFirst_URE1. For ten switches, 13 patches were not identified. ReliabilityFirst_URE1 completed additional research that revealed nine patches for three IDS assets that were issued, but not identified, and therefore not timely assessed for applicability or implemented. The root cause of this violation related to the management practices of workforce management through ineffective training and poor asset and configuration management. ReliabilityFirst_URE1 personnel responsible for evaluating and applying patches did not fully understand their responsibilities and were confused about the data and format required to use the patch management tool because they were ineffectively trained. Additionally, the four firewalls were not properly monitored, and 13 patches for 10 switches were not properly inventoried and documented, which shows poor asset management.	CIP-007-1	R3; R3.1; R3.2	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
10	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. ReliabilityFirst_URE1's infrastructure design provides layers of security that minimize the risk of an impact. Th devices in question were in a demilitarized zone and or/behind secure firewalls. ReliabilityFirst_URE1's standard change control policies and procedures require verification of multiple security controls to provide a baseline level of security that further minimizes the risk. For the redundant syslog server in particular, cyber security controls testing was being performed, but the documentation was not adequately completed. The logs for the redundant syslog server were sent to a primary device as well as the redundant device. The primary device was logging normally and would have collected th required logs to monitor the Bulk Electric System.	when ReliabilityFirst_URE1 first failed to complete cyber security controls testing on the devices at issue	Mitigation Plan completion
11	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All of the assets affected sit behind several layers of protection. ReliabilityFirst_URE1 utilizes a secure network architecture and employs a layered security model to protect these assets. Each of these assets has been deployed with their own demilitarized zone, which is separate from both the business and control networks. The assets themselves have been hardened against attack, are not Internet-facing assets, and reside behind several layers of protection and firewalls. To reach these assets, a would-be attacker would have to first infiltrate 2 to 3 layers of firewalls before even being able to attempt an attack on the devices. These security controls mitigate the risk posed to the Bulk Electric System.	when the first patch was not applied	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
10	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) developed training materials on cyber security controls testing, including requirements around the performance of such tests and documentation of evidence; 2) identified impacted personnel, including personnel responsible for installing new cyber assets and performing significant changes to existing cyber assets for which cyber security controls testing would be required pursuant to CIP-007 R1; 3) delivered training to impacted personnel; and 4) performed a quality assurance assessment on a sample set of significant changes to verify that cyber security controls tests are being performed and documented in accordance with company processes and procedures.	12/31/2014	4/7/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-007 R1 compliance history to be an aggravating factor in the penalty determination.
11	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) verified which in-scope cyber assets are included in the automated patch identification process; 2) verified what software installed on in-scope cyber assets is configured appropriately in the patching tool; 3) conducted an extent of condition analysis to verify the scope of the issue; 4) performed all outstanding security patch assessments and scheduled applicable patches for implementation; 5) decided to enhance the existing ReliabilityFirst_URE1 security patch management program or adopt the patch management program to prevent recurrence; 6) delivered training on the revised or adopted security patch management procedures to all impacted ReliabilityFirst_URE1 personnel; and 7) performed a quality assurance assessment of ReliabilityFirst_URE1 patches to ensure that patches were appropriately identified, assessed, and scheduled.	6/5/2015	8/17/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-007 R3 compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
12	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014014172	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R5. As a result of an internal assessment, ReliabilityFirst_URE1 identified instances in which passwords for certain accounts were not changed at least annually. In total, ReliabilityFirst_URE1 identified 51 accounts where passwords were not updated within 365 days as required by CIP-007-3a R5. In particular, ReliabilityFirst_URE1 identified instances where personnel designated as backups or emergency users had not logged into their accounts within the last 365 days. ReliabilityFirst_URE1 does not have the technical capability to automatically disable these accounts upon password expiration. Therefore, once a password expires, the account user is prompted to change the password when he or she logs in for the first time after the previous password has expired. In the identified cases, because the users had not logged into their accounts within the last 365 days, the user had also not been prompted to change their account password within the last 365 days as the Standard requires. As a result, the passwords associated with these accounts expired without being changed within the annual time frame. Of the 51 accounts where passwords were not updated within 365 days, 20 involved accounts on the Energy Control System, 25 involved user accounts on the regulated private network domain, and six involved accounts on the security event monitoring application. If users had attempted to access any of the accounts more than 365 days after their last access attempt, the user would have been prompted to make a password change when the user logged in, thus ensuring that a password change would have occurred the next time the account was used. The root cause of this violation related to the management practice of reliability quality management through ineffective and incomplete controls for monitoring the age of an account's password. The process ReliabilityFirst_URE1 relied upon to ensure passwords were updated, counting on users to periodically access their accounts and then update their passwords, was defective and incomplete because many backup users did not access their accounts annually. ReliabilityFirst_URE1 did not have in place additional controls, independent of a user accessing his or her account, which would ensure that passwords were changed at least once every 365 days.	CIP-007-3a	R5	Lower	Severe
13	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013761	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R6. ReliabilityFirst_URE1 identified a set of Electronic Access Control and Monitoring Assets (EACMS) that were not properly configured to log at the time of installation. ReliabilityFirst_URE1 implemented a security event monitoring system. This system is used to meet the technical requirement for logging, monitoring, and alerting under CIP-005 R3, CIP-007 R5.2.3, and CIP-007 R6.5. ReliabilityFirst_URE1 has used this system to collect asset logs, alert on specific event criteria, and provide reports for event monitoring since its installation. ReliabilityFirst_URE1 identified that when the system was installed, eight hardened appliances were not capturing their own logs and not forwarding their internal asset logs to a log repository. The root cause of this violation related to the management practice of reliability quality management. ReliabilityFirst_URE1's weak procedural controls for the installation of new assets, which did not provide sufficient detailed steps to ensure that a device was capturing its own logs prior to the completion of the installation, caused ReliabilityFirst_URE1 to not identify that eight devices were not capturing their own logs.	CIP-007-3a	R6	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
12	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Many of the passwords for these accounts have redundant controls, password complexity and length requirements, in place. The users with access to these accounts were up-to-date with their annual training and personnel risk assessments. Additionally, monitoring controls are in place to alert the appropriate CIP asset owners when multiple failed login attempts are made. For an outside intruder to exploit these accounts, the intruder would need to infiltrate several layers of firewalls or obtain physical access to a protected Physical Security Perimeter before the intruder could gain access to these accounts. ReliabilityFirst_URE1 has also determined that the accounts in question have not been used to gain access, interactive or otherwise, to any CIP assets since the passwords expired.	when ReliabilityFirst_URE1 was required to comply with the Standard	the date ReliabilityFirst_URE1 finished updating or deleting all overdue and expired passwords
13	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The assets that do not log have a minimal impact to the Bulk Electric System because they have no direct control function or telemetry monitoring of critical assets. The assets in question were in a demilitarized zone and/or behind secure firewalls. The assets have a very limited number of accounts with access, and interactive access to these assets occurs infrequently. Unauthorized access to the assets would not allow any access to any other NERC Cyber asset, Critical Cyber Asset, EACMS, or Protected Cyber Asset. Although a compromise of the assets would place the logging of specific CIP assets at risk, ReliabilityFirst_URE1 has monitoring and alerting of other CIP assets in place that is designed to identify anomalous behavior. Lastly, ReliabilityFirst_URE1's infrastructure design provides layers of security that minimize the risk of an impact.	when ReliabilityFirst_URE1 first implemented the security event monitoring system	the date ReliabilityFirst_URE1 confirmed that all assets were forwarding all of their logs appropriately

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
12	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) identified all user accounts for which passwords were not changed within the annual timeframe; 2) determined which accounts are necessary and need to remain active and which accounts need to be deleted; 3) required password changes on user accounts that need to remain active; 4) deleted user accounts that do not need to remain active; 5) developed a procedure for monitoring user account password ages. This procedure was documented and contained steps for monitoring account password ages approaching 365 days, to ensure that passwords are changed within the required timeframe, and for disabling accounts if necessary; 6) developed and scheduled a plan for implementation; 7) delivered training to all personnel responsible for performing tasks under the new procedure; and 8) communicated implementation of the new procedure to all impacted personnel.	1/27/2015	8/7/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's CIP-007 R5 compliance history to be an aggravating factor in the penalty determination.
13	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) implemented measures to ensure the identified security event monitoring assets are forwarding their logs; 2) defined process improvements such as enhancements to existing processes and controls and the development of new processes and controls to ensure that new EACMS devices are properly configured to log at the time of installation; 3) developed and delivered training to impacted personnel on process improvements; 4) developed a plan to transition to a significant change testing program; 5) developed and delivered training to impacted personnel on the change testing program; 6) communicated implementation of change testing program; and 7) performed a quality assurance assessment on a sample set of newly installed devices to verify that the change testing program is being implemented as intended.	6/29/2015	10/26/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
14	ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (ReliabilityFirst_URE 1)	NCRXXXXX	RFC2014013757	Settlement Agreement	ReliabilityFirst_URE1 submitted a Self-Report to ReliabilityFirst stating that it was in violation of CIP-007-3a R9. ReliabilityFirst_URE1 identified instances where it did not have sufficient evidence to establish the timely completion of annual reviews and approvals of documentation specified in CIP-007-3a R9 as subject to annual review obligations. ReliabilityFirst_URE1 identified 31 procedures that are subject to the CIP-007 R9 annual review requirement. ReliabilityFirst_URE1's program defines annually as once per calendar year and no more than 16 months between events or activities. Seven of the 31 identified procedures did not indicate clear evidence of having an annual review with approval that met the ReliabilityFirst_URE1 annual criteria. The seven procedures are as follows: (1) CIP Security Alert and System Monitoring Procedures; (2) Corporate Security Account Management Procedure; (3) Corporate Security CIP Change Control Procedure; (4) CIP Access Authorization Procedure; (5) Energy Control System (ECS) Testing Environment; (6) Security Incident Response Process; and (7) Shared Accounts Procedure. The root cause of this violation related to the management practices of verification and asset and configuration management. There was no built-in check to verify that a review was completed and approval obtained for each procedure that was scheduled to be updated. Additionally, the procedures and associated documents did not have a clear owner, an individual responsible to make sure that the update was properly completed. This lack of a clear owner meant the procedures were not effectively inventoried or monitored.	CIP-007-3a	R9	Lower	High
15	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2015014708	Settlement Agreement	SERC_URE1 submitted a Self-Certification stating that it was in violation of CIP-007-3a R3.1. SERC_URE1 failed to assess security patches for applicability within 30 days of availability for Cyber Assets within the Electronic Security Perimeter (ESP). SERC_URE1 went operational with a new energy management system (EMS). SERC_URE1 used an automated tool that assimilated available security bulletins, which SERC_URE1 used to assess security patches for applicability, but SERC_URE1 omitted service packs from inclusion in the tool. As a result, SERC_URE1 did not review, assess or install two service packs and did not include subsequent security patches affiliated with the two service packs in the automated tool. Thus, SERC_URE1 did not assess 22 security patches within 30 days of availability. The release dates of these security patches ranged during a two and a half year period. After discovering the issue, SERC_URE1 determined that seven patches were not applicable and 15 patches were required. This issue affected 28.3% of the total Cyber Assets within the SERC_URE1 CIP program. SERC_URE1 discovered this issue when an employee saw a patch in the corporate patch queue that did not show up in the EMS patch queue. The employee was assisting in a corporate patching issue when he learned of the issue. While conducting an extent-of-condition review, SERC_URE1 subject matter experts found a second application with security patches that SERC_URE1 had not assessed within 30 days of availability. While installing the new EMS, SERC_URE1 installed the application on a single non-critical Cyber Asset within the ESP. SERC_URE1 had not used the application since installation and failed to assess the applicability of three patches that were available. In total, SERC_URE1 failed to assess 25 security patches for applicability within 30 days of their availability. The root cause of the first issue was that the SERC_URE1 security patch assessment process lacked specificity on how to manage potential security patches specific to service packs. The root cause of the second issue was that the individuals responsible for reviewing patches did not know that the second	CIP-007-3a	R3; R3.1	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
14	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The missed annual reviews posed minimal risk because all lists and diagrams that relate to CIP operational concerns were separately reviewed and approved annually. Additionally, processes in the original document were not materially modified from the processes that existed during the timeframe of the missed annual reviews. ReliabilityFirst_URE1 also independently assesses compliance through formal self-assessment processes and not by the installation of updates. Updates are completed to meet the specific CIP obligation that requires the update and to identify areas of improvement. Lastly, all updates were completed, though not always on time or with complete documentation.	when ReliabilityFirst_URE1 could not provide evidence that the seven procedures had an annual review	the date ReliabilityFirst_URE1 completed, and documented, annual reviews with approval for the seven procedures
15	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1's failure to assess security patches for applicability within 30 days of being available could have allowed malicious individuals to exploit known vulnerabilities for an extended period. However, SERC_URE1 requires the use of a screening firewall, a jump host solution, two-factor authentication, and a proxy server, to gain remote access to Cyber Assets within the ESP, limiting the ability of an external individual to exploit any vulnerabilities on the Cyber Assets at issue. SERC_URE1 centrally monitored logs from the implicated Cyber Assets and any anomalous events would generate an alert to the appropriate response personnel. SERC_URE1 has not had any incidents during the violation period in which the cause is known to be malicious, suspected to be malicious, or unknown. The Cyber Assets at issue were within secured ESPs and Physical Security Perimeters with controlled access. All personnel with access to the Cyber Assets at issue had received cyber security training and had a valid personnel risk assessment.	when SERC_URE1 installed a new EMS without ensuring that all applicable security patches had been assessed	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
14	$25,000 (for RFC2014013763, RFC2014014186, RFC2014013840, RFC2014014535, RFC2014013760, RFC2014013839, RFC2014014167, RFC2014013759, RFC2014013758, RFC2014014094, RFC2014014172, RFC2014013761, and RFC2014013757)	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) developed an inventory of ReliabilityFirst_URE1 CIP-007 documentation; 2) reviewed the inventory to assess annual review completion dates and determined which documents, if any, were not reviewed within the annual review timeframe; and 3) conducted the following annual review and ensured that all inventory documents were reviewed and approved within the annual review timeframe.	12/31/2014	4/7/2015	Neither Admits nor Denies	ReliabilityFirst_URE1 has been highly cooperative throughout the entire enforcement process as it voluntarily provided ReliabilityFirst with an abundance of information regarding the Violations in a manner that was detailed, well-organized, and timely. ReliabilityFirst_URE1's level of cooperation has been exemplary and ReliabilityFirst awards a significant amount of mitigating credit for this cooperation to encourage this sort of response by other Registered Entities in the future. ReliabilityFirst considered ReliabilityFirst_URE1's compliance history and determined there were no relevant instances of noncompliance.
15	$5,000	Self-Certification	To mitigate this violation, SERC_URE1: 1) retroactively identified the missing security patches; 2) documented, evaluated for applicability, tested, and implemented if applicable, each missing patch; 3) modified the procedure on reviewing, logging, and tracking security patches to include greater details about how, where, and what to look for when reviewing security patches; 4) conducted a self-review of the modified patch process material as well as instruction from third-party support with subject matter experts to ensure that the patch processes are fully understood; and 5) modified its change management process and associated change management form to include a step for identifying all applications on devices associated with the change.	3/20/2015	12/10/2015	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's compliance history and determined there were no relevant instances of noncompliance.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
16	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2015014764	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE2 was in violation of CIP-005-3a R2.2. SERC_URE2 failed to enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter (ESP) at all access points to the ESP. SERC_URE2 removed a failed Cyber Asset from within the ESP. During the decommissioning of the Cyber Asset, SERC_URE2 did not eliminate the firewall rules for traffic to the Cyber Asset from the three ESP firewalls associated with that specific Cyber Asset. This mistake permitted ports on each of the three firewalls to remain open and available. SERC_URE2 performed an extent-of-condition and discovered two additional port issues. In the first additional issue, SERC_URE2 removed an application but left open a port in error. In the second additional issue, SERC_URE2 discovered another Cyber Asset that had a firewall rule in place for a port that was not required. SERC_URE2 originally thought that the port was required for a time sync with the global positioning clocks, but upon further review, SERC_URE2 determined that the Cyber Asset at issue was only used for frequency and not time. SERC_URE2 closed all of the ports upon discovery. The root cause of this violation was a failure by SERC_URE2 personnel to follow the existing change control and configuration management procedures.	CIP-005-3a	R2; R2.2	Medium	Severe
17	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2015014604	Settlement Agreement	SERC sent SERC_URE2 an audit detail letter notifying it of an upcoming Compliance Audit. SERC_URE2 submitted a Self-Report stating that it was in violation of CIP-006-3c R2.2. SERC_URE2 failed to ensure that the Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP) were afforded the protective measures specified in CIP-003 R6 and CIP-007 R2, R4, R5, R6, and R8. SERC later determined that this violation extended back to Version 1 of the Standard. Prior to the Compliance Audit, SERC_URE2 retained a third-party consultant to conduct audit preparations. The consultant determined that SERC_URE2 failed to afford its physical access control system (PACS) door controllers with the protections referenced in CIP-006-1 R1.8 since the date of mandatory compliance. Specifically, SERC_URE2 had not: (a) established what ports and services were necessary for normal and emergency operations and disabled a single port that was not required for normal and emergency operations as required by CIP-007 R2; (b) requested a Technical Feasibility Exception (TFE) for the inability for account passwords to meet the complexity requirements specified in CIP-007 R5.3; and (c) requested a TFE due to the inability to run anti-virus and malware prevention software as required by CIP-007 R4. In addition to the issues noted in the Self-Report, SERC determined that SERC_URE2 had not: (a) established a configuration management benchmark documentation for the PACS door controllers and did not include them in the change control form for CIP-003 R6; (b) requested a TFE for the PACS door controllers that were not capable of monitoring for cyber security events as required by CIP-007 R6. SERC_URE2 believed that the door status monitoring performed by the PACS door controllers that would be communicated to the PACS server constituted status monitoring and eliminated the need for a TFE for the PACS door controllers; and (c) included the PACS controllers in its cyber vulnerability assessment (CVA) as required by CIP-007 R8. The door controllers at issue had no accounts, but did have ports and services. The vendor who conducted the annual SERC_URE2 CVAs did not include the PACS controllers. A different vendor conducted a CVA and identified the issue. However, SERC_URE2 failed to follow-up and reconcile the noted issue at that time. During the CVA,	CIP-006-1	R1; R1.8	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
16	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SERC_URE2's failure to disable open ports and services that were not required for normal or emergency operations could allow a malicious individual to gain access to and control of Critical Cyber Assets (CCAs), potentially leading to a loss of control or visibility over SERC_URE2's portion of the BPS. However, the firewall rules for the initial issue that were not required were associated with a previous access control appliance that was on a subnet by itself. Once SERC_URE2 removed the previous access control appliance, there was no Cyber Asset on the subnet that could have used the ports or seen authentication requests from the firewall. The ports for the application in the first additional issue were all outbound ports, limiting the potential attack vectors, reducing access opportunities, and restricting vulnerabilities. The port open to the devices in the second additional issue was open only to a trusted de-militarized zone and other restricted subnets. Any outsider attempting to connect to a device involved in the second additional issue using the port would not get a response because the device was not actually providing that service.	when SERC_URE2 enabled the firewall rules that permitted the open port that was not required	Mitigation Plan completion
17	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2's failure to afford the PACS devices all of the applicable protective measures specified in CIP-006-1 R1.8 could have allowed unauthorized individuals to gain physical or electronic access to Critical Cyber Assets or non-critical Cyber Assets and potentially damage or manipulate those devices. However, for the first issue, the PACS door controllers are firmware-based appliances and the unauthorized reconfiguration or modification of these devices would be difficult. For the second issue, SERC_URE2 needed the open port and simply omitted it from the baseline documentation. SERC_URE2 had placed the involved PACS server on a separate Electronic Security Perimeter (ESP) subnet and the firewall blocked the open port from any inbound access. Finally, all the PACS devices were protected within ESPs and PSPs.	when the Standard became mandatory and enforceable on SERC_URE2	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
16	$20,000 (for SERC2015014604, SERC2015014635, SERC2015014762, and SERC2015014764)	Compliance Audit	To mitigate this violation, SERC_URE2: 1) removed the access list and rules in the firewall that open ports to/from and allow authentication via the former IP address of the Cyber Asset; 2) provided training to appropriate personnel to emphasize the need to consider other devices, especially firewalls, when removing an asset from service; and 3) removed the firewall rules formerly used by the application and the rules opening the port to the devices.	5/19/2015	11/16/2015	Neither Admits nor Denies	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition to its mitigating activities, SERC_URE2 has completed or agreed to complete the following additional actions: a. SERC_URE2 adopted a cyber and physical security objective as part of SERC_URE2's strategic plan. SERC_URE2 staff briefed the Board regarding the initial progress in meeting the objective and will provide subsequent written reports to the Board on a monthly basis and in-person verbal updates to the Board on a quarterly basis. b. SERC_URE2 has budgeted funds to replace existing Remote Terminal Units (RTUs) without password protection capability with RTUs that have password protection to restrict configuration changes and firmware updates. SERC_URE2 expects to replace the RTUs over a two year period. c. In addition to performing the required cyber vulnerability assessment (CVA), SERC_URE2 will perform a cyber vulnerability review on non-CIP assets. The review will include the above active CVA as well as intrusion risk assessments on IT and operations technology networks.
17	$20,000 (for SERC2015014604, SERC2015014635, SERC2015014762. and SERC2015014764)	Self-Report	To mitigate this violation, SERC_URE2: 1) established a baseline to document required ports and services for door controllers per CIP-003 R6; 2) scanned all controllers to ensure only those required ports are open; 3) filed TFEs for controllers for CIP-007 R4 and R5.3; 4) provided reminder training to affirm the need to document all cyber devices in CIP scope, including those performing limited specific tasks; 5) filed TFE for controllers for CIP-007 R6; 6) completed a CVA of the controllers to mitigate failure to include them in prior years; 7) modified the CVA process form to include instructions to ensure that all CIP relevant Cyber Assets are covered by the test plan before it is approved; 8) revised the ports baseline in the configuration management database (CMD) to justify a port being open for the PACS server; 9) conducted an annual CVA to ensure all ports are properly documented in the CMD and prevent recurrence of undocumented ports; and 10) document the PACS server log messages and implement automated alerting when those logs occur.	12/31/2015	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC_URE2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit. SERC considered SERC_URE2's compliance history to be an aggravating factor in the penalty determination. In addition to its mitigating activities, SERC_URE2 has completed or agreed to complete the following additional actions: a. SERC_URE2 adopted a cyber and physical security objective as part of SERC_URE2's strategic plan. SERC_URE2 staff briefed the Board regarding the initial progress in meeting the objective and will provide subsequent written reports to the Board on a monthly basis and in-person verbal updates to the Board on a quarterly basis. b. SERC_URE2 has budgeted funds to replace existing Remote Terminal Units (RTUs) without password protection capability with RTUs that have password protection to restrict configuration changes and firmware updates. SERC_URE2 expects to replace the RTUs over a two year period. c. In addition to performing the required cyber vulnerability assessment (CVA), SERC_URE2 will perform a cyber vulnerability review on non-CIP assets. The review will include the above active CVA as well as intrusion risk assessments on IT and operations technology networks.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
18	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2015014635	Settlement Agreement	SERC sent SERC_URE2 an initial notice of a Compliance Audit. SERC_URE2 submitted a Self-Report stating that it was in violation of CIP-006-3c R5. SERC_URE2 failed to implement technical and procedural control for monitoring physical access at all access points to the Physical Security Perimeters (PSPs) 24 hours a day, 7 days a week. An SERC_URE2 operator went on shift during the night without his or her access badge, which the operator had forgotten at home. The previous shift operator who was being relieved permitted the operator access to the PSP where the operators worked. However, after being left alone for the shift, the operator left the PSP for approximately four minutes and blocked the door open to permit a return. When the door was blocked open, the security console at SERC_URE2 received a "door held open" alarm but the security personnel failed to respond or react to the alarm because the security personnel believed the alarm resulted from cleaning staff with authorized unescorted access. Instead, the security personnel acknowledged the alarm to silence it. SERC_URE2 had documented procedures for how to manage access for personnel with lost or forgotten access badges, as well as procedures for how security personnel must handle entry alarms once received. Annual training also covered this aspect as well as the necessity to maintain the integrity of the PSP. The procedures and training further specified that any anomalies encountered not addressed within existing training or procedures should be brought to the attention of a CIP representative immediately for proper resolution. The procedure for lost or stolen access cards contained the precautionary language about undocumented situations. The instant issue in which a night-shift operator worked alone within a PSP was not documented in the procedure. The operator's supervisor was made aware that the operator had forgotten their badge at the start of the shift pursuant to the SERC_URE2 procedure. The supervisor attempted to contact the employee to discuss having the employee return home to retrieve the badge or have a family member deliver it to the worksite, but found the operator had already left the control center without the badge. The root cause of this violation was a failure to follow established SERC_URE2 procedures.	CIP-006-3c	R5	Medium	Severe
19	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2015014762	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE2 was in violation of CIP-007-3a R3.1. SERC_URE2 subsequently identified additional instances of violations with CIP-007 R3. SERC_URE2 failed to document the assessment of security patches and security upgrades for applicability within 30 calendar days of the availability of the patches or upgrades for several Cyber Assets within the Electronic Security Perimeter (ESP). A firmware update became available. SERC_URE2 received and was aware of the update within 30 days of its release. However, SERC_URE2 did not realize that the firmware update was for security issues. SERC_URE2 personnel thought the update was solely related to operational functionality bug fixes because "security update" was not prominent in the bulletin. As a result, SERC_URE2 took no action on the release and did not assess its applicability to Cyber Assets within the ESP. SERC_URE2 had three affected Cyber Assets in service. SERC_URE2 discovered a second issue and notified SERC. SERC_URE2 was investigating a software program within its energy management system (EMS) for broader use within its CIP program when it discovered that SERC_URE2 had not assessed a security patch that had been issued for the software program within 30 days of the security patch being released. SERC_URE2 included the software program, which is used for monitoring, in the EMS deployment and deployed the software program in a basic functioning state on one of two domain controllers in the primary control center and one of two domain controllers in the back-up control center. SERC_URE2 never configured the software program for use or activated any functionality within the EMS application. After discovery of the second issue, SERC_URE2 did a full extent-of-condition for all installed software applications and patch review issues. SERC_URE2 submitted an expansion of scope to SERC after it discovered a set of firmware-based switches that it did not assess for possible security updates after SERC_URE2 deployed them with the new EMS. SERC_URE2 deployed these two switches in order to isolate the EMS system from any external networks in the event an intrusion was detected. SERC_URE2 could operate the switches manually, but they also had an automated	CIP-007-3a	R3; R3.1	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
18	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SERC_URE2's failure to immediately investigate a "door held open" alarm caused by an SERC_URE2 operator propping the door open resulted in an approximately four-minute period during which the PSP was unoccupied and no security personnel investigated or guarded the PSP. Further, the operator's workstation was unlocked during this period. This violation could have allowed an unauthorized individual to gain physical access to Critical Cyber Assets (CCAs) without being challenged, enabling that individual to damage, destroy, or misuse the CCAs. However, the workstation within the PSP could only directly operate elements of the BPS if an individual with the appropriate credentials logged on and took action. The operators in this location lacked such credentials. In addition, the PSP in question is within the SERC_URE2 headquarters building, which has locked doors that are operated by approved security badge card readers. SERC_URE2 reviewed video footage and confirmed that no one entered the PSP during this incident.	when the security console received the alarm for "door held open" but failed to respond immediately	when the operator returned to the PSP and secured the PSP door
19	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2 's failure to assess security patches within 30 days of availability could have left vulnerabilities on Cyber Assets available for exploit by malicious individuals for an extended period. However, for the first and third issues, the Cyber Assets at issue were firmware-based appliances, making the ability to modify or affect the operating parameters of the Cyber Assets difficult. For the second issue, the application involved was active but unutilized. The affected Cyber Assets did not communicate outside the ESP because the firewall would block any external connections, and the Cyber Assets resided within a secured ESP and Physical Security Perimeter with monitoring and logging enabled.	when SERC_URE2 installed the new EMS with the monitoring application included	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
18	$20,000 (for SERC2015014604, SERC2015014635, SERC2015014762, and SERC2015014764)	Self-Report	To mitigate this violation, SERC_URE2: 1) distributed a reminder email to personnel with unescorted access to PSPs reminding personnel of the importance of contacting their supervisor or CIP Standard owner for any situations where an appropriate response is unknown or unclear; 2) disciplined the employee that initiated the incident and dismissed the security staff that failed to investigate the alarm; 3) minimized nuisance and false alarms related to PSP monitoring by placing a longer delay between opening and initiating of the door held open alarm and retraining the cleaning crews to be more mindful of the door alarms to avoid these types of alarms; 4) installed a dedicated recording/monitoring system for cameras monitoring PSP access points; 5) reviewed, and if applicable updated, physical security policies to address additional scenarios encountered which contributed to violations; 6) reviewed, and if applicable, updated training programs to ensure personnel with unescorted access to PSPs understand what steps to take when procedures are unclear or situations are not addressed by a specific procedure; and 7) had staff complete refresher training on the procedures related to alarm response for personnel charged with responding to alarms.	6/5/2015	9/8/2015	Neither Admits nor Denies	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC_URE2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit. In addition to its mitigating activities, SERC_URE2 has completed or agreed to complete the following additional actions: a. SERC_URE2 adopted a cyber and physical security objective as part of SERC_URE2's strategic plan. SERC_URE2 staff briefed the Board regarding the initial progress in meeting the objective and will provide subsequent written reports to the Board on a monthly basis and in-person verbal updates to the Board on a quarterly basis. b. SERC_URE2 has budgeted funds to replace existing Remote Terminal Units (RTUs) without password protection capability with RTUs that have password protection to restrict configuration changes and firmware updates. SERC_URE2 expects to replace the RTUs over a two year period. c. In addition to performing the required cyber vulnerability assessment (CVA), SERC_URE2 will perform a cyber vulnerability review on non-CIP assets. The review will include the above active CVA as well as intrusion risk assessments on IT and operations technology networks.
19	$20,000 (for SERC2015014604, SERC2015014635, SERC2015014762, and SERC2015014764)	Compliance Audit	To mitigate this violation, SERC_URE2: 1) applied the firmware release with the security update to the device; 2) conducted security patch evaluation training; 3) applied the latest patch for the software program; 4) create a support account for IT personnel to access patches; and 5) reviewed all software and firmware in the configuration management database to ensure patches are being reviewed and document the patch source.	8/14/2015	9/11/2015	Neither Admits nor Denies	SERC reviewed SERC_URE2's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. In addition to its mitigating activities , SERC_URE2 has completed or agreed to complete the following additional actions: a. SERC_URE2 adopted a cyber and physical security objective as part of SERC_URE2's strategic plan. SERC_URE2 staff briefed the Board regarding the initial progress in meeting the objective and will provide subsequent written reports to the Board on a monthly basis and in-person verbal updates to the Board on a quarterly basis. b. SERC_URE2 has budgeted funds to replace existing Remote Terminal Units (RTUs) without password protection capability with RTUs that have password protection to restrict configuration changes and firmware updates. SERC_URE2 expects to replace the RTUs over a two year period. c. In addition to performing the required cyber vulnerability assessment (CVA), SERC_URE2 will perform a cyber vulnerability review on non-CIP assets. The review will include the above active CVA as well as intrusion risk assessments on IT and operations technology networks.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
20	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2015015164	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE4 was in violation of CIP-009-3 R1. SERC_URE4's recovery plan did not address the minimum requirements called for by CIP-009 R1. SERC later determined that this issue dated back to Version 1 of the Standard. SERC_URE4's recovery plan for Critical Cyber Assets (CCAs) did not meet the requirements of CIP-009-3 R1 because it did not specify the required actions in response to events or conditions of varying severity or duration that would activate the recovery plan and did not define the roles and responsibilities of responders. Instead, SERC_URE4 utilized a broader business recovery or business continuity type plan for CIP-009-3 R1 with a focus on the redundancy of the Cyber Assets at both the primary control center as well as the back-up control center, noting the ability to move between the two sites in the event of a site failure. In the event of a total failure of both sites, SERC_URE4 cited manual operations and a reliance on neighboring entities. In addition, the recovery plan does not contain references to the recovery of Cyber Assets, other than guidance on where replacement Cyber Assets could be purchased and how to find the proper data restoration media. The root cause of this violation was a misunderstanding by SERC_URE4 on what was required to be in the CIP-009 R1 recovery plan for CCAs. Specifically, SERC_URE4 compliance staff failed to understand that recovery plans must include all criteria laid out by the standard/requirement and not just what would be included in the business continuity plan. SERC_URE4 misinterpreted the standard believing the term "recovery" was indicating recovering operations at the backup site, rather than recovering Cyber Assets.	CIP-009-1	R1	Medium	Severe
21	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2015015166	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE4 was in violation of CIP-005-3a R1.5. SERC_URE4 did not afford four electronic access control and monitoring (EACM) Cyber Assets the protective measures specified in CIP-007-3a R5.3.2 because the EACM Cyber Assets could not technically enforce password strength (a combination of alpha, numeric, and “special” characters) and SERC_URE4 did not submit a request for a Technical Feasibility Exception (TFE). During the on-site audit, SERC_URE4 discovered that its network intrusion detection system (NIDS), consisting of four servers classified as EACM Cyber Assets, did not technically enforce password complexity. The password module that SERC_URE4 used had technical limitations that prevented it from properly managing the complexity of the root account password. Upon discovery, SERC_URE4 disclosed this issue to the SERC audit team on site and initiated immediate efforts to remediate. The four EACM Cyber Assets at issue were put into service when SERC_URE4 implemented a new energy management system (EMS). The root cause of this violation was a misunderstanding by SERC_URE4 of the technical abilities and limitations of modules used to enforce password complexity requirements.	CIP-005-3a	R1; R1.5	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
20	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE4's failure to specify the required actions in response to events or conditions of varying duration and severity and to define the roles and responsibilities of responders in its recovery plan for CCAs could have delayed the recovery of CCAs after an event that compromised the operation of those CCAs. However, SERC_URE4 had a high-level business continuity plan that identified the ability to continue operations through back-up sites and use manual operations and rely on neighboring entities in the event of a total failure of the primary and backup sites. SERC_URE4 did not need to use the recovery plan during the duration of the violation.	when the Standard became mandatory and enforceable on SERC_URE4	Mitigation Plan completion
21	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SERC_URE4's failure to enforce password complexity on the EACM devices could allow a malicious individual to guess or crack the passwords and gain control of the EACM devices, giving them unauthorized access to Critical Cyber Assets (CCAs) However, the EACM devices did not have direct control of any CCAs and are not used to meet CIP logging requirements. SERC_URE4 had procedural controls in place to ensure use of passwords with the required complexity. SERC_URE4 installed the EACM devices to enhance its security posture and came into audit scope due to the classification of the system as an EACM. This violation lasted less than five months.	when SERC_URE4 implemented the EACM devices and used a password module that did not technically enforce the complexity requirements on root account passwords	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
20	$20,000 (for SERC2015015164, SERC2015015165, SERC2015015166, and SERC2015015167)	Compliance Audit	To mitigate this violation, SERC_URE4: 1) updated its procedures to reflect how it will address the recovery of individual CCAs following failover; and 2) trained appropriate personnel regarding all procedural changes, including formal reinforcement training with energy management system backup and recovery procedures.	8/10/2015	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE4's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
21	$20,000 (for SERC2015015164, SERC2015015165, SERC2015015166, and SERC2015015167)	Compliance Audit	To mitigate this violation, SERC_URE4: 1) found another application that would apply the complexity requirement to the root account; and 2) installed and tested the application.	8/7/2015	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE4's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
22	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2015015165	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE4 was in violation of CIP-006-3c R2. SERC_URE4 failed to afford physical access control system (PACS) devices the protective measures specified in CIP-007-3a R5.2.3 by documenting shared account usage in all cases. SERC_URE4 had a policy that required individuals who used shared accounts to manually document the shared account use on a log sheet. SERC discovered that an employee used a shared administrator account and failed to log the usage of the shared account for the PACS. The actual log-on and usage of the shared account was captured in the events logging for the PACS but did not document the individual that used the account. On the date of the discovery, SERC_URE4 initiated an extent of condition review comparing the actual events logs from the PACS servers to the manual spreadsheet over the previous 90 days and included all shared accounts in service across the CIP environment. SERC_URE4 did not find any additional failures to log usage of shared accounts on the PACS servers. Approximately three months after the failed log, SERC_URE4 implemented an automated solution to log shared account usage on all shared accounts The root cause of this violation was a human performance failure. The individual using the shared account in question failed to complete the required manual log of account usage.	CIP-006-3c	R2; R2.2	Medium	Severe
23	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2015015167	Settlement Agreement	During a Compliance Audit, SERC determined that SERC_URE4 was in violation of CIP-007-3a R1.3. SERC_URE4's testing procedure did not sufficiently address documentation of test results, which caused SERC_URE4 to not consistently document and retain test results. During the Compliance Audit, SERC reviewed several significant changes in which SERC_URE4 lacked evidence showing that it conducted testing. SERC_URE4's documented testing procedures lacked the details needed to obtain consistent evidence that testing occurred. SERC_URE4 did not provide evidence that testing had consistently occurred. The root cause of this violation was a failure by SERC_URE4 to have detailed enough testing procedures to ensure that SERC_URE4 staff would consistently test and maintain evidence of testing.	CIP-007-3a	R1; R1.3	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
22	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE4's failure to accurately log usage of a shared account could hinder an investigation of who made certain changes to a system or whether such access was unauthorized. However, The PACS Cyber Assets were secured within a Physical Security Perimeter (PSP), with restricted and logged access. This issue was the only noted occurrence over the previous 90-day period. SERC_URE4 did not identify any unauthorized modifications or changes to the PACS.	when a SERC_URE4 employee using the shared account failed to log the usage on the manual log entry form	Mitigation Plan completion
23	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SERC_URE4's failure to demonstrate testing of all significant changes for adverse impacts to existing cyber security controls could have resulted in implemented changes disabling or removing existing security controls, increasing the risk of unauthorized access to Critical Cyber Assets or the introduction of security vulnerabilities. However, SERC_URE4 had a port scanning tool set to run every 10 hours to detect and alert on any ports changes that were made. SERC_URE4 secured all Cyber Assets within an established Electronic Security Perimeter and a Physical Security Perimeter.	the day after SERC_URE4 completed its Mitigation Plan for the prior violation	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
22	$20,000 (for SERC2015015164, SERC2015015165, SERC2015015166, and SERC2015015167)	Compliance Audit	To mitigate this violation, SERC_URE4: 1) updated its process to use an automated log system created in-house that runs a log on script at user log on that detects if the account is in the "Shared Account" group; and 2) trained appropriate personnel regarding all procedural changes, including formal reinforcement training on automated procedures.	8/7/2015	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE4's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination.
23	$20,000 (for SERC2015015164, SERC2015015165, SERC2015015166, and SERC2015015167)	Compliance Audit	To mitigate this violation, SERC_URE4: 1) developed a new test procedure for security controls; and 2) trained appropriate personnel regarding all procedural changes, including formal reinforcement training with security controls testing procedure.	8/10/2015	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE4's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE4's compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
24	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2015014963	Settlement Agreement	SERC determined that SERC_URE3 was in violation of CIP-006-3c R2.2. SERC_URE3 failed to identify physical access control systems (PACS) door controllers as PACS devices and therefore failed to afford these Cyber Assets the protective measures specified in R2.2. SERC later determined that the violation extended back to Version 1 of the Standard and Requirement, when the Requirement was found at CIP-006-1 R1.8. SERC_URE3 failed to consider two components serving the back-up control center as part of the PACS. As a result, SERC_URE3 had no evidence that it afforded the components the protective measures required by CIP-006-3c R2.2. The components were Cyber Assets that fulfilled the function of an intelligent door controller, but were also a part of the physical lock mechanism. The access control components were firmware-based and stored badge information, verified that the badge was authorized, communicated to the lock mechanism to unlock the door, and stored logs of each badge presentation. Individuals could access the controller ports of these intelligent door controllers from outside the Physical Security Perimeter (PSP) because the controller ports were located on the exterior of the door. SERC_URE3 conducted any programming of these devices from the exterior of the PSP. SERC_URE3 believed that because the Cyber Assets were a part of the actual physical lock, they fell under the exclusionary statement within CIP-006-3c R2 that provides: "Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall … be afforded the protective measures specified in … [the list of Requirements found in CIP-006-3c R2]" However, because the intelligent door controllers fulfilled the PACS obligation of authorizing and logging access, they were a primary part of the PACS system and SERC_URE3 was required to provide them with the protective measures listed in CIP-006-3c R2.2. Therefore, while SERC_URE3 properly applied the exclusion to the physical badge reader and lock components, SERC_URE3 should not have extended the exclusion to the Cyber Assets that stored badge information, verified badge authorization, and communicated to the lock mechanism to unlock the door.	CIP-006-1	R1; R1.8	Lower	Severe
25	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2015014966	Settlement Agreement	SERC determined that SERC_URE3 was in violation of CIP-006-3c R1.1. SERC_URE3 failed to ensure all Cyber Assets within an Electronic Security Perimeter (ESP) resided within a completely enclosed (six-wall) Physical Security Perimeter (PSP). SERC later determined that this violation extended back to Version 1 of the Standard. A SERC_URE3 Critical Asset substation had dial-up remote access to its Critical Cyber Assets (CCAs) but no external routable remote access. However, the substation also had CCAs within it that used routable protocols internal to the substation ESP to communicate. SERC_URE3 interpreted CIP-006-3, Section D.1.5.2, "For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall not be required to comply with Standard CIP-006-3 for that single access point at the dial-up device" to apply not only to the single access point but to all CCAs at the substation. As a result, SERC_URE3 concluded that the substation did not require a PSP because the CCAs within it were only accessible via dial-up remote access. While the exception found in Section D.1.5.2 is applicable to the "single access point at the dial-up device," SERC_URE3 had CCAs within the substation that used routable protocols. Thus, SERC_URE3 should have established a PSP to protect the CCAs at the substation that used routable protocols. SERC_URE3 took actions, including removing the dial-up access to some CCAs, that resulted in reclassifying the substation as a Critical Asset that had no CCAs. The root cause of this violation was SERC_URE3's misinterpretation of the CIP-006 Standard, specifically Section D.1.5.2. SERC determined that SERC_URE3 was in violation of CIP-006-1 R1.1 because SERC_URE3 failed to ensure all Cyber Assets within an ESP resided within a completely enclosed (six-wall) PSP.	CIP-006-1	R1; R1.1	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
24	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's failure to properly protect the Cyber Assets that authorized access to its PSP for more than six years could have permitted access by unauthorized personnel who could modify or add to existing access permissions, giving them physical access to Critical Cyber Assets. However, the PACS devices in question were within a secured building that had video monitoring sent to the energy control center guard and the central monitoring station. The device involved was firmware-based and had no firmware upgrades issued during the violation, limiting potential security concerns.	when the Standard became mandatory and enforceable on SERC_URE3	Mitigation Plan completion
25	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's failure to secure all Cyber Assets within an ESP within an established six-wall PSP could allow unauthorized individuals to gain physical access to CCAs without being detected and allow those individuals to alter or compromise the Cyber Assets or their data. SERC_URE3 failed to provide the required protection to the CCAs for almost five years. However, SERC_URE3 had physical access controls in place for the substation, which included a locked perimeter fence, on-site security personnel making regular periodic security checks, a restricted access control house that used a badge reader which contained all involved Cyber Assets, a request and approval process for obtaining card access to the control house, and access logging through the badge reader. No known security breaches of this site occurred during the violation.	when the Standard became mandatory and enforceable on SERC_URE3	when SERC_URE3 took actions that resulted in the reclassification of the site as a Critical Asset with no CCAs

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
24	$45,000 (for SERC2015014963, SERC2015014966, SERC2015014968, and SERC2015014970)	Compliance Audit	To mitigate this violation, SERC_URE3: 1) installed, tested, and implemented a PACS which includes the standby control center, at this facility; and 2) conducted communication and training of the PACS at the standby control center.	4/1/2016	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's CIP-006-1 R1.8 compliance history to be an aggravating factor in the penalty determination.
25	$45,000 (for SERC2015014963, SERC2015014966, SERC2015014968, and SERC2015014970)	Compliance Audit	To mitigate this violation, SERC_URE3: 1) removed dial-up remote access to the facility involved; 2) in preparation for CIP V5, identified the facility where dial-up remote access previously existed as a facility housing Bulk Electric System Cyber Systems with a Medium Impact rating; 3) installed, tested, and implemented a physical access control systems (PACS) at this facility; and 4) conducted communication and training on the PACS at this facility.	4/1/2016	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC determined that SERC_URE3's CIP-006 R1 compliance history should not serve as a basis for aggravating the penalty.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
26	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2015014968	Settlement Agreement	SERC determined that SERC_URE3 was in violation of CIP-005-3a R3. SERC_URE3 failed to document its security monitoring processes to detect and alert for attempts at or actual unauthorized accesses when conducting manual reviews. SERC later determined that the violation extended back to Version 1 of the Standard. SERC_URE3 utilized an automated tool and rule-based aggregation to monitor and log access to the Electronic Security Perimeter (ESP) firewalls as well as to alert for attempts at or actual unauthorized accesses. However, SERC_URE3 depended on manual log reviews to detect and alert for attempts at or actual unauthorized access into the ESP through the firewall. Although SERC_URE3 had an isolated network and limited access avenues into the ESP, SERC_URE3's assessment of access was limited to a manual periodic review of access logs and SERC_URE3 did not have a documented process for how to conduct these manual log reviews or what to look for in the reviews. As a result, SERC_URE3 relied on experienced personnel to conduct this manual review by using professional judgment, looking for anything that appeared out of the ordinary, and any unauthorized or unusual traffic through the firewall would have been readily evident to them. If personnel saw any unusual traffi during this review, they would conduct a more in-depth review of a sample of logs. However, without a documented process for conducting these manual reviews, SERC_URE3 could not ensure consistent implementation of the manual review process or consistent documentation of the results of those reviews. The root cause of this issue was SERC_URE3's misunderstanding of the Standard and Requirement, specifically the requirement to document its process. SERC determined that SERC_URE3 was in violation of CIP-005-1 R3 because SERC_URE3 failed to implement and document, where technically feasible, security monitoring processes to detect and alert for attempts at or actual unauthorized accesses to the ESP.	CIP-005-1	R3	Medium	Severe
27	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2015014970	Settlement Agreement	SERC determined that SERC_URE3 was in violation of CIP-009-3 R1. SERC_URE3 failed to create a sufficient recovery plan for Critical Cyber Assets (CCAs). SERC_URE3 revised its recovery plan document, making the document to be more of a broad business recovery or business continuity-type plan. The document focused on the redundancy of the involved systems at both the primary control center as well as the back-up control center (both Critical Assets) and the ability to move between the two sites in the event of a site failure at either. The document did not specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plans and did not define the roles and responsibilities of responders. The root cause of this violation was SERC_URE3's lack of understanding of what CIP-009-3 R1 required. SERC determined that SERC_URE3 was in violation of CIP-009-3 R1 because SERC_URE3 failed to create a sufficient recovery plan for CCAs.	CIP-009-3	R1	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
26	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's failure to have documented processes for the manual review of all attempts at or actual unauthorized access to the ESP could result in inconsistent manual reviews of logs, potentially allowing an intrusion attempt or actual intrusion to go undetected for an extended period. However, SERC_URE3's overall network topology used layered firewalls outside of the ESP, restricting traffic to the firewall. SERC_URE3 had policies in place that prohibited interactive sessions through the ESP access points, limiting potential attack vectors. SERC_URE3 limited external connectivity and did not permit direct Internet accessible communication, which provided SERC_URE3 with known traffic patterns that would allow any unexpected or anomalous traffic to be readily apparent to an experienced log reviewer.	when the Standard became mandatory and enforceable on SERC_URE3	Mitigation Plan completion
27	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's failure to specify the required actions in response to events or conditions of varying duration and severity and to define the roles and responsibilities of responders in its recovery plan for CCAs could have delayed the recovery of CCAs after an event that compromised the operation of those CCAs. However, SERC_URE3 had high-level business continuity plans to permit continuation of operations through a back-up site. SERC_URE3 did not need to use the recovery plan during the violation.	when SERC_URE3 revised its recovery plan	Mitigation Plan completion

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
26	$45,000 (for SERC2015014963, SERC2015014966, SERC2015014968, and SERC2015014970)	Compliance Audit	To mitigate this violation, SERC_URE3: 1) researched and purchased a new ESP firewall; 2) developed criteria for logging and alerting; 3) tested filtering of firewall logs and alerting capabilities of the new firewall; 4) implemented security information and event management email alerts for loss of logging by the firewall; 5) developed a backup manual process to review firewall logs. To aid in the transition to CIP V5, the review will be conducted as prescribed in NERC CIP-007-5, Part 4.4; and 6) completed training on the manual review process.	4/1/2016	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3's compliance history and determined there were no relevant instances of noncompliance.
27	$45,000 (for SERC2015014963, SERC2015014966, SERC2015014968, and SERC2015014970)	Compliance Audit	To mitigate this violation, SERC_URE3: 1) developed updated recovery plans to meet the requirements of CIP Version 5. These plans include a higher level of detail related to the recovery of specific assets, the events or conditions and severity that would activate the plan, and roles and responsibilities; and 2) completed communication and training of the updated recovery plans.	4/1/2016	TBD	Neither Admits nor Denies	SERC reviewed SERC_URE3's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE3 compliance history and determined there were no relevant instances of noncompliance.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 31, 2016

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP16-__-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

NERC respectfully requests that the Commission accept this Spreadsheet NOP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
2	Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2015015369	Settlement Agreement	FRCC_URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R2. Security patches were inadvertently installed on Physical Access Controls Systems (PACS) devices, consisting of servers and workstations, without following the CIP-007-3 R3 patching procedures, as required in CIP-006-3 R2.2. A FRCC_URE1 Senior Systems Programmer was implementing a change order to install patches on the non-CIP test server. The patching tool required the programmer to select the devices that would receive the patches. However, the programmer inadvertently included the CIP PACS devices along with the selection of the non-CIP test server. The patches themselves did not create issues, the issue was that they were not procedurally applied per CIP-007-3 R3. The programmer immediately realized the mistake, but was unable to stop the patches from being deployed since the patching tool had no cancelation feature. The programmer attempted to log in directly to the PACS devices to cancel the patches, but they had already been applied. The programmer tested the functionality to ensure that the patches had not caused to function improperly. Two weeks after the inadvertent patch installation, the programmer opened a scheduled change order to re-apply the same patches to the PACS devices, to ensure that all of patches were properly applied (procedurally) and that necessary CIP-007-3 R3 pre- and post-scans were performed. The patches were successfully reapplied. The patching procedure verified that all applicable patches had been applied to the devices and completed the remaining steps of the patching process. FRCC_URE1 performed a root cause analysis and determined that the primary root cause was the programmer's screen had a visibility issue that made it difficult to see the devices being selected in the patch management tool. Additionally, the procedure should have included a validation step requiring verification that the patches were matched with the correct device, prior to applying and the patching tool should not be able to patch both test and production environments simultaneously. The patch groups should have been separated within the patching tool.	CIP-006-3c	R2; R2.2	Medium	Severe
3	Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2015015368	Settlement Agreement	FRCC_URE1 submitted a Self-Report stating that it was in violation of CIP-005-3a R1.4. FRCC_URE1 failed to afford protections as required by CIP-005-3a R1.4 for non-CCA devices: Integrated Lights Out (iLOs), and Modular Smart Arrays (MSAs) that were connected to an Electronic Security Perimeter (ESP). A network analyst submitted a request to identify and add the servers and the storage arrays (which were to be added to an ESP) to the asset management database. However, the analyst neglected to include the iLO devices associated with the servers to the database. The network analyst submitted an additional request (a change order) to configure a network switch to enable ports to allow communications to the devices in the ESP network. However, again the iLO devices were not included in the request as required in CIP-003-3 R6. The non-CCA devices where connected to the network upon approval of the request. It wasn't until several months later that the correct requests were opened to properly add the iLO devices to the asset management database, and to complete the remaining onboarding tasks that did not take place under the original request to configure the network switch. FRCC_URE1 performed a root cause analysis for this noncompliance and determined that the root causes were inadequate preventative controls that allowed the network analyst to overlook the iLO devices when submitting the necessary change orders and a lack of training and clear procedures. The network analyst did not understand that by connecting the devices to the ESP, CIP protections were required regardless of the fact the operating system had not been installed on the associated servers that the devices support.	CIP-005-3a	R1; R1.4	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
2	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS).The inadvertent patching process mistake could have potentially compromised the functionality of the PACS system or the PACS server could have become unresponsive. However, if the PACS system or server were to have been rendered unresponsive, the controls at the doors (allowing/disallowing access) would still function, and logs would still be produced. Once the devices became responsive again, the logs and alerts would be sent to the central PACS server. During the time the devices are unresponsive, the guards would not receive alarms concerning the door status for a Propped Door or Forced Door event. However, the guards would know that the application was not responsive, and would activate the established compensating procedures for such a situation. Additionally, the patches in question had been applied to other devices on the corporate network without issue before they were applied on the PACS devices. No harm is known to have occurred.	when the programmer inadvertently installed patches	when the programmer ensured that all of the applicable patches had been applied to the devices and completed the remaining steps of the patching process
3	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The servers that the iLOs are attached to are still powered off and have no operating system installed on them, and the MSAs have not been utilized for data storage. The devices were not reachable (when communications were established to the iLO devices during the approved change process) due to firewall rules in place, which meant the devices were unable to communicate during the period of noncompliance. No harm is known to have occurred	when the iLO devices were connected to the network without having the required protection	when the iLO devices were added to the asset management database

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	$35,000 (for FRCC2015015366, FRCC2015015368, and FRCC2015015369)	Self-Report	To mitigate this issue, FRCC_URE1: 1) ensured that all of the applicable patches had been applied to the devices and completed the remaining steps of the patching process on; 2) the CIP Senior Manager sent out communications (to vice president of information technology & chief information officer) on situational awareness related to NERC compliance; 3) changed the patching tool to separate the specific production and test PACS environments into individual scan results. This will prevent inadvertent device selection for the PACS environment in the future; 4) changed the patching tool to separate all other NERC production and test environments into individual scan results. This will prevent inadvertent device selection for all other NERC environments; 5) separated NERC and non-NERC virtual patching consoles. This will prevent corporate (non-NERC) patching from inadvertently being applied to NERC devices; 6) changed resolution settings/replace monitor as necessary for all patching programmers; 7) revised the Security Patch Management Program and associated desk level procedures (DLPs) to include greater awareness of the impacts of the processes to NERC compliance, add a validation step for applying the patches, and delineate the necessary steps to follow in the event of a process failure, including a strict timeline for resolution of the issue; and 8) performed refresher training to applicable SMEs, patching implementers, and asset owners on the revised patching process and associated DLPs.	12/18/2015	2/8/2016	Neither Admits nor Denies	FRCC reviewed FRCC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. FRCC considered FRCC_URE1's compliance history to be an aggravating factor in the penalty determination.
3	$35,000 (for FRCC2015015366, FRCC2015015368, and FRCC2015015369)	Self-Report	To mitigate this issue, FRCC_URE1: 1) properly on-boarded (procedurally processed) the devices as NERC devices. The Manager of Network Technology reviewed the two-step onboarding/change management process with network analyst; 2) communication was sent from the CIP Senior Manager, (vice president of information technology & chief information officer) on situational awareness related to NERC compliance; 3) specifically address iLOs in the New NERC Asset form; and 4) facilitated a combined NERC change management session between IT techs, IT Security and Asset Management to clarify the procedures in the NERC Change Management Process relative to the timing of onboarding NERC devices and the associated change type to use and communicated any clarifications to applicable team members.	12/23/2015	2/8/2016	Neither Admits nor Denies	FRCC reviewed FRCC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. FRCC considered FRCC_URE1's CIP-003-3 R6 and CIP-006-3c R2 compliance history involving similar conduct to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
4	Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2015015366	Settlement Agreement	FRCC_URE1 submitted a Self-Report stating that it had an issue of CIP-005-3a R2, 2.2. FRCC_URE1 inadvertently configured Electronic Security Perimeter (ESP) firewall rules that enabled ports and associated services on devices within a demilitarized zone (DMZ) network that were not required for normal or emergency operations or monitoring to communicate through a NERC ESP access point. The incorrect firewall rules were in-place for a period of seven days. A security analyst implemented a change to configure firewall rules to allow network access to a new DMZ testing environment in preparation for an upgrade of the Energy Management System (EMS). To allow internal access to the new DMZ, a new firewall rule was defined that allowed eight new servers in a DMZ to access the corporate network. During the implementation of the rules in the change, the security analyst discovered that he had omitted a rule allowing traffic out of the new DMZ environment The analyst corrected the omission by adding a new rule to allow outbound communication from the new DMZ to the corporate network. However, the rule configuration also inadvertently allowed communication into the existing ESP for EMS, which shares the same perimeter firewall with the new DMZ. According to the firewall logs, the first traffic to cross the firewall from the new DMZ network into the ESP occurred when the senior network and systems analyst activated the interface. The traffic was blocked when the emergency change was implemented. A security analyst discovered the problem as they were implementing security measures on the eight new servers in the new DMZ. Upon confirmation of the rule configuration, the analyst then initiated an emergency change to stop all traffic to the ESP from the servers in the new DMZ. The traffic was blocked when the emergency change was implemented. FRCC_URE1 performed a root cause analysis for this noncompliance and determined that the root causes were a lack of preventive tools or controls in place to prevent this type of error and the analyst involved relied too much upon institutional knowledge, rather than existing procedures.	CIP-005-3a	R2 R2.2	Medium	Severe
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
19										

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
4	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). FRCC_URE1 inadvertently allowed communication into the existing ESP for EMS, which shared the same perimeter firewall with the new DMZ, and therefore could have exposed its network system to malicious cyber attacks and affected FRCC_URE1's operations. The potential risk to the BPS was minimized because the point of attack would have to been to access one of the servers, and to gain access, credentials would be required. There were only four applicable individuals with credentials, all are long-term trusted employees that have current NERC physical and interactive remote access. The servers were in the various initial stages of being onboard and not all of the devices were connected for the entire duration. The only software installed on the servers was the operating system, and applicable patches were applied prior to onboarding the devices. The only type of communications allowed into the ESP environment by the rule were from the new access restricted (future NERC EMS test environment) DMZ. No interactive access from the new network was made in to the ESP environment and there were no corporate assets, people, and/or any other Energy Control Center DMZs that could access the ESP while these rules were in place. Additionally, the new DMZ network and the EMS ESP share a Physical Security Perimeter (PSP). There were no workstations with access, but there were new servers in the DMZ allowed access by the rule. The four individuals had credentials with access to servers in the new DMZ environment. However, those credentials did not allow access into the systems within the ESP. Neither upgrades to devices nor updates to an individual's credentials would have allowed access. No harm is known to have occurred.	when the analyst configured firewall rules to allow network access to a new DMZ testing environment	when traffic was blocked and the emergency change was implemented
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
4	$35,000 (for FRCC2015015366, FRCC2015015368, and FRCC2015015369)	Self-Report	To mitigate this issue, FRCC_URE1: 1) corrected the inadvertent firewall rule; 2) sent communications from the CIP Senior Manager, (to vice president of information technology & chief information officer) on situational awareness related to NERC compliance; 3) created a new desk level procedure (DLP), which includes peer review, for firewall rule changes; and 4) trained applicable team members on the new DLP.	1/13/2016	2/8/2016	Neither Admits nor Denies	FRCC reviewed FRCC_URE1 internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. FRCC considered FRCC_URE1's CIP-005-3a R2 compliance history to be an aggravating factor in the penalty determination.
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							

Attachment A-2

May 31, 2016, Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered Entity**	**NCR_ID**	**NERC Violation ID #**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
20										
21										
22										
23										
24										
25										
26										
27										

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
20			
21			
22			
23			
24			
25			
26			
27			

	N	O	P	Q	R	S	T
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified**	**"Admits," "Agrees/Stipulates,"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
20							
21							
22							
23							
24							
25							
26							
27							

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of 11 violations of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred twenty-five thousand dollars ($225,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SERC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SERC2014013657	CIP-002-3	R3	High/ Severe	SR	Minimal	$225,000
SERC2014013877	CIP-005-1	R1	Medium/ Severe	CA	Moderate	
SERC2014013910	CIP-005-3a	R4	Medium/ Severe	CA	Minimal	
SERC2014014396	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014014403	CIP-006-3c	R8	Medium/ Severe	SR	Minimal	
SERC2014013881	CIP-007-3a	R5	Medium/ Severe	CA	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SERC2014014274	CIP-007-3a	R5	Medium/ Severe	SR	Minimal	$225,000
SERC2014013438	CIP-007-3a	R6	Lower/ Severe	SR	Moderate	
SERC2014013765	CIP-007-3a	R6	Lower/ Severe	SR	Minimal	
SERC2014013767	CIP-007-3a	R8	Medium/ Severe	SR	Moderate	
SERC2014013766	CIP-009-3	R5	Lower/ Severe	SR	Moderate	

SERC2014013657 CIP-002-3 R3 - OVERVIEW

SERC determined that URE did not develop a comprehensive list of all Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset in three instances. The first instance was due to URE's failure to document the asset on its network drawings upon commissioning or within 90 days. For the second and third instances, URE business units did not provide required data elements to the responsible personnel and were inconsistent in their classification of devices.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE's failure to document all CCAs on its CCA lists increased the risk that it would not afford those CCAs all the protections of the CIP Standards, which could allow a malicious individual to disrupt or misuse CCAs and thereby impair URE's situational awareness of the BPS. In the first instance, the device did not have control functions to operate key assets within the Critical Asset. The device communicated to the control center though a protected network that had monitoring and logging enabled. In addition, the device only provided analog and digital status updates with limited control functionality for reclosing breakers and backup ground relay protection. For the second and third instances, the CCAs that URE omitted from the CCA list had the required CIP security protections. Lastly, URE protected all of the CCAs URE omitted from the CCA list within Electronic Security Perimeters (ESPs) and Physical Security Perimeters (PSPs), and access was limited to authorized personnel who had taken cyber security training and had valid personnel risk assessments (PRAs).

SERC determined the duration of the violation to be from when URE commissioned the first device without identifying it as a CCA through when the senior manager updated and approved the CCA list.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove all control capabilities from the device so it is currently in a monitoring state only providing analog and digital statuses;
2. perform a walk-down to verify there are no additional CCAs that were installed and not properly identified;
3. perform a review of the Cyber Asset list to determine all of the Critical Asset locations;
4. perform a review of all ESP diagrams to confirm all CCAs are captured;
5. establish a standard operating procedure for identifying whether projects affect Critical Assets;
6. perform a review of the current information captured on all CCAs;
7. perform a review of the current process and identify updates to the current process for updating the CCA list;
8. identify the owners in the business unit/support groups responsible for maintaining the attributes on CCAs in their respective areas on a quarterly basis;
9. modify the CCA list to reflect the required fields needed for classification of the asset;
10. update the process to include the steps for the business unit/support group owners to follow; and
11. communicate the revised process to the business unit/support group representatives.

URE certified that it had completed its Mitigation Plan.

SERC2014013877 CIP-005-1 R1 - OVERVIEW

SERC determined that URE did not afford the protective measures specified in CIP-007 R3 to Cyber Assets used in the access control and/or monitoring of the ESP by failing to assess security patches on firewalls within 30 days of availability in two instances. URE had a subscription service with the firewall vendor for timely notification via email, however it had not received security patch updates from the vendor for several years due to an incorrect email address in the vendor site. URE did not follow up with the vendor or implement a secondary verification process to ensure that it received security patch notifications.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to assess security patches on the electronic access control and monitoring (EACM) devices at issue and subsequent failures either to install the security patches or implement compensating measures increased the risk that the EACM devices could be compromised, which could allow unauthorized electronic access to CCAs located within the ESP. Nevertheless, URE had an in-depth defense strategy of protection in which an intruder would first have to gain access through corporate firewalls to attempt access to the EACM devices at issue and avoid detection by an intrusion detection system. Further, the firewalls in question are located within PSPs. There were no known Cyber Security Incidents during the duration of the violation.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE assessed the missed security patches.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. verify that it is receiving security alerts from identified support vendors;
2. establish a communication link to receive advisory alerts;
3. update its IT security vulnerability management procedure;
4. identify the people who require training on the updated IT security vulnerability management procedure;
5. create training on the updated IT security vulnerability management procedure; and
6. deploy training on the IT security vulnerability management procedure.

URE certified that it had completed its Mitigation Plan.

SERC2014013910 CIP-005-3a R4 - OVERVIEW

SERC determined that URE did not document the plan to mitigate vulnerabilities identified during the annual Cyber Vulnerability Assessment (CVA). URE conducted its annual CVA and failed to identify that the network group or the firewall ruleset were no longer required because it had removed the devices from the network. URE's CVA process did not have enough detail to examine the deployed network objects or rulesets thoroughly.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to complete its CVA action plan to remove objects from the firewall rule group could allow unauthorized traffic to traverse the ESP. Nevertheless, the firewall rule containing

this group object was an outward-bound rule that only allowed communication out of the ESP and did not allow communication into the ESP. Further, the associated IP addresses were not associated with a network within the current ESP. The network group or configured firewall ruleset would not have allowed traffic to traverse the firewall and gain access to CCAs.

SERC determined the duration of the violation to be from the date when the network object and firewall ruleset were no longer required, through when URE implemented the approved change management removing the devices from the network object.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review and update the asset disposal and redeployment procedures;
2. create and deploy a change control and asset disposal or redeployment specific training program for personnel;
3. create a sub-task for the team to remove the machine name from the asset database; and
4. create sub-task for the system access sub-team to remove any specific firewall rules associated with a server to release the IP address for use by another system.

URE certified that it had completed its Mitigation Plan.

SERC2014014396 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not implement the technical and procedural controls for monitoring physical access at all access points to the PSP 24 hours a day, seven days a week. URE discovered that one of the PSP access points failed to provide "door forced open" and "door held open" alarms to the centralized security command center because of an equipment malfunction at the door contact.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor physical access at all PSP access points 24 hours a day, seven days a week could allow attempts at unauthorized physical access to CCAs within a PSP to go undetected. Nevertheless, the PSP door contacts were not functional for, at most, eight days. In addition, URE personnel are present in the PSP in question 24 hours a day, seven days a week. The PSP in question is located within a facility that has security on-site 24 hours a day, seven days a week with roving patrols. Upon discovering this issue, URE immediately deployed a security officer at the door until it repaired the door later that day. Although the door failed to provide the required alarms, it remained locked and only allowed authorized personnel access. URE performed a walk-down at all of its PSPs and determined that there were no other similar issues.

SERC determined the duration of the violation to be from the date the door contacts failed, through when URE repaired and tested the door contacts.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training to the protective service employees responsible for PSP commissioning and validations;
2. update its PSP inspection checklists;
3. issue an emergency work order to repair the door contact; and
4. perform operability testing and return the door to full functionality.

URE certified that it had completed its Mitigation Plan.

SERC2014014403 CIP-006-3c R8 - OVERVIEW

SERC determined that URE did not perform testing and maintenance of all physical security mechanisms for one site on a cycle no longer than three years. URE utilizes a manual tool for tracking the maintenance and testing schedule. URE discovered that personnel mistakenly removed the PSP from view within the tool. Personnel had originally scheduled to remove the PSP from CIP scope prior to the next scheduled maintenance test.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to perform testing and maintenance of physical security mechanisms at least every three years could lead to URE being unaware of malfunctioning physical access control mechanisms, potentially allowing unauthorized individuals to gain physical access to CCAs. Nevertheless, URE secured the site with locking hardware and card readers and monitored 24 hours a day, seven days a week during the issue. In addition, the Cyber Assets deployed within the site in question were "low" upon implementing the CIP Version 5 impact rating criteria. URE performed additional operability testing on two occasions and determined that the physical access control systems were still operating as designed.

SERC determined the duration of the violation to be from three years and one day after URE conducted the last testing and maintenance of the physical security mechanisms at the site in question, through when URE updated its risk-based assessment methodology (RBAM) and removed the site from the Critical Asset list.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. decommission the PSP as a NERC CIP site;
2. conduct maintenance and testing for the site;
3. audit the existing maintenance and testing schedule to ensure all NERC CIP sites are listed and dates are accurate;
4. update the existing two procedural documents that support CIP-006-3c R8 to remove outdated information and incorporate current processes;
5. redesign the maintenance and testing tracking spreadsheet to include additional information needed for tracking and coordination with the business units;
6. retire and replace legacy/local procedures with new enterprise-wide procedures to ensure consistency in performing CIP-006-3c R8 maintenance and testing; and
7. retire the existing maintenance and testing checklist and revise to meet requirements of the new enterprise-wide procedures and ensure the document is complete and complies with CIP-006-3c R8.

URE certified that it had completed its Mitigation Plan.

SERC2014013881 CIP-007-3a R5 - OVERVIEW

SERC determined that URE did not change all default passwords on certain CCA and Critical Assets prior to deploying them within the ESP and failed to change each password at least annually. URE personnel were not familiar with the various levels of accounts available on the CCAs. Therefore, it did not know the accounts in question were present.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to change default passwords prior to putting CCAs in service could allow malicious individuals with knowledge of the default passwords to gain unauthorized electronic access to the CCAs. URE's subsequent failure to ensure that it changed passwords on the CCAs annually increased the risk that malicious individuals could compromise old passwords to gain unauthorized electronic access to the CCAs. Nevertheless, in order to access the default accounts, an individual would first have to login to the first-level account. Remote access to the CCAs was limited to individuals who had two-factor authentication configured and had the appropriate software application for successful interaction with the CCA. Remote access was not possible to the Cyber

Assets. The Cyber Assets were located within PSPs, which URE secures with badge readers and monitors access to 24 hours a day, seven day a week.

SERC determined the duration of the violation to be from the date when URE put the CCAs into service without changing the default passwords, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the current settings procedure to include language that outlines the need for an annual password reset for the specific devices and the steps to perform a password reset;
2. create a procedure that outlines the steps to be taken to perform an annual password update for the specific devices via remote access;
3. update the asset database list item field to include direction that the specific passwords need to be reset annually;
4. identify the list of people who required training and train on the updated setting procedure, the procedure for performing a password reset via remote access, and the change to the list item field to include direction that passwords need to be reset annually;
5. change all specific accounts' passwords during its annual password update;
6. perform a review of all assets to determine if any assets did not have an automatic password reset performed within 365 days;
7. create and document a procedure for performing a manual review of assets to determine whether an automated password reset has been performed; and
8. update the commissioning process document to direct the team to commission assets with unique asset names that have not been previously used.

URE certified that it had completed its Mitigation Plan.

SERC2014014274 CIP-007-3a R5 - OVERVIEW

SERC determined that URE did not implement its policy to secure shared accounts within seven days following personnel changes. URE did not configure its automated tool to change shared account passwords automatically. Therefore, URE was required to change the passwords manually. URE had a procedure in place stating the necessity to change shared account passwords manually, however URE personnel failed to follow it.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to change a password in a timely manner could have permitted unauthorized access to CCAs potentially resulting in damage and/or degradation of BPS reliability. Nevertheless, URE removed the logical access and physical access for the employee in question on the day of departure and changed the account password within ten days of the employee's departure. Prior to the voluntary departure, the employee was in good standing with URE, was current on training, and had a current PRA. URE verified that no changes occurred on the devices in question during the issue.

SERC determined the duration of the violation to be from eight days after the employee left URE and no longer required access to the shared account in question, through when URE manually changed the shared account password.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. manually change the shared account password;
2. identify individuals responsible for updating passwords to shared accounts; and
3. distribute the account management process to identified individuals to reeducate them on the importance of updating passwords to share accounts as documented in this policy.

URE certified that it had completed its Mitigation Plan.

SERC2014013438 CIP-007-3a R6 - OVERVIEW

SERC determined that URE did not implement automated tools or organizational process controls to monitor system events related to cyber security for all Cyber Assets within the ESP. Personnel did not understand the CIP logging requirements for the devices and thus did not configure them in the centralized security log-monitoring tool. Instead, personnel thought the devices were technically incapable of logging and would require filing TFEs. URE discovered additional CCAs that were not logging system cyber security events during its extent of condition review. URE personnel did not realize that for the second group of CCAs, it had to request that its vendor create rules to allow communication with the logging tool.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor system events related to cyber security for the devices could have resulted in a security breach going undetected or impaired a response to a possible or actual security breach. An undetected security breach could render CCAs inoperable, resulting in the loss of monitoring and control of the BPS. Nevertheless, the CCAs have no direct control over the BPS.

Access to the Cyber Assets involved in this violation is limited to individuals with authorized physical or electronic access rights, and URE protects the Cyber Assets within an ESP and a PSP. In addition, URE has an intrusion detection system that monitors the network and alerts personnel in the event of unusual activity. URE did not discover or detect any cyber security events, Misoperations, emergencies, or other adverse consequences because of this violation.

SERC determined the duration of the violation to be from the date URE began installing the devices without implementing automated tools or organizational process controls to monitor system events related to cyber security, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify the resources that would require re-training of the asset commissioning process;
2. update documentation to include testing;
3. identify list of personnel requiring training on the updated procedures;
4. update and submit TFEs for relevant devices;
5. test devices; and
6. notify staff and conduct training.

URE certified that it had completed its Mitigation Plan.

SERC2014013765 CIP-007-3a R6 - OVERVIEW

SERC determined that URE did not implement automated tools to monitor system events related to cyber security for all Cyber Assets within the ESP and did not submit a request for a TFE to SERC that documented compensating measures. URE discovered CCAs at a single facility that were technically incapable of monitoring or logging cyber security events. URE maintained evidence from the vendor that the CCAs were not capable of logging or monitoring events related to cyber security. Nevertheless, URE failed to submit a request for a TFE to SERC that documented compensating measures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to submit a request for a TFE documenting compensating measures for CCAs that were technically incapable of monitoring or logging cyber security events could have led URE to not document or implement compensating measures to protect the devices at issue, which could result in a security breach going undetected. Nevertheless, URE had implemented compensating measures

that included intrusion detection and protection systems monitoring for abnormal or malicious network traffic that were in place when it commissioned the CCAs. URE deployed CCAs within a PSP and ESP behind multiple firewalls. URE did not discover or detect any cyber security events, Misoperations, emergencies, or other adverse consequences because of this issue.

SERC determined the duration of the violation to be from the date when URE commissioned the CCAs that were technically incapable of monitoring or logging cyber security events without submitting a request for a TFE that documented compensating measures, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the facility from scope with a new RBAM utilizing new criteria; and
2. implement a new TFE program and train the TFE audience.

URE certified that it had completed its Mitigation Plan, and SERC verified that URE had completed all mitigation activities.

SERC2014013767 CIP-007-3a R8 - OVERVIEW

SERC determined that URE did not perform CVAs of all Cyber Assets within its ESPs at least annually. URE discovered CCAs within its Cyber Assets that contained a connection with the supervisory control and data acquisition (SCADA) wide area network. URE personnel did not understand that the CVA requirements applied to these Cyber Assets connected to the CCA.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to perform a CVA on Cyber Assets in its facilities could have left the Cyber Assets residing within ESPs open to potential security threats and compromise for an extended period. Nevertheless, URE logically separated the local area network from the SCADA network, and the Cyber Assets resided within secured ESPs and PSPs. Remote access to the Cyber Assets from outside the ESP required two-factor authentication. In addition, URE's electronic access and control monitoring devices did not identify any malicious activity during the violation that would have affected the involved Cyber Assets. URE restricted access to the Cyber Assets to authorized individuals with completed PRAs and cyber security training.

SERC determined the duration of the violation to be from the date it commissioned the first site, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review documents listing all of the existing ports;
2. perform a CVA on all Cyber Assets during the annual walk-downs;
3. initiate testing of full-time CVA scans in a test lab; and
4. draft engineering configuration/settings and designs to implement a new CVA process.

URE certified that it had completed its Mitigation Plan.

SERC2014013766 CIP-009-3 R5 - OVERVIEW

SERC determined that URE did not annually test information essential to recovery that is stored on backup media to ensure that the information is available for the CCAs at one facility. URE's subject matter expert had misunderstood the requirement, believing it was sufficient to create frequent backup tapes throughout the year, instead of testing the tapes to ensure the information was readable. URE's disaster recovery procedure implemented at the site required annual testing of the backup media.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to test backup media necessary to recover CCAs could result in it being unaware that the information was corrupted, possibly delaying or preventing the restoration of CCAs. Nevertheless, this violation affected a single site and thus would have a limited effect in the event that URE needed to recover the CCAs at the site. URE performed frequent backups of the information necessary to recover the CCAs and performed monitoring of the backup system. No Misoperations, emergencies, or other adverse consequences occurred during the period of the violation.

SERC determined the duration of the violation to be from the date URE commissioned the CCAs at the facility without testing the information essential to recovery to ensure it was available, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. gather lessons learned and conduct training to ensure individual subject matter experts understand the requirements and processes that are outlined to be compliant with this requirement; and

2. perform training and lessons learned gathered with individuals reviewing work management tickets that are created to initiate the completion of this requirement.

URE certified that it had completed its Mitigation Plan.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of two hundred twenty-five thousand dollars ($225,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC determined the compliance history should serve as an aggravating factor;
2. SERC considered certain elements of URE's internal compliance program (ICP) as a mitigating factor in the penalty determination. Specifically, URE's ICP is documented and readily available to its employees on its intranet. A URE compliance group reviews its ICP on an annual basis, which reports within URE's compliance department to ensure independence from the operations and engineering departments that must comply with the NERC Standards. URE employees receive quarterly newsletters to ensure awareness of ethics and compliance issues and annual CIP training. URE employees are also required to understand all corporate policies and procedures, including those related to compliance, and are subject to discipline, up to and including termination, for violating those policies. Nevertheless, SERC reduced ICP credit due to URE's compliance history and inability to prevent recurrence of CIP issues.
3. URE voluntarily self-reported eight of the violations; however, five of the Self-Reports came after notice of an upcoming Compliance Audit, and therefore did not receive mitigating credit;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. six of these violations posed minimal risk and five violations posed moderate risk and did not pose a serious or substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of two hundred twenty-five thousand dollars ($225,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Prior to starting settlement discussions, SERC initiated meetings with URE compliance staff and middle management to discuss the high number of URE violations and the issues SERC was seeing with URE's compliance efforts. SERC management met with URE senior management after settlement discussions began to continue the discussion of SERC's concerns. To address SERC's concerns, URE met with SERC after reaching a settlement agreement to inform SERC of a comprehensive action plan that included the following elements:

1. The creation of an internal board, to ensure adequacy of cause and extent of condition analyses and review effectiveness of mitigation plans;

2. Enhanced oversight by an internal committee, along with enhanced reporting to provide members with immediate notification of possible violations;

3. Enhanced mitigation plan tracking at the enterprise level to allow for regular status reporting;

4. Quarterly meetings with SERC to discuss progress and solicit feedback;

5. The review and enhancement of URE's communication plan to educate business continually on the company's approach to ensure NERC compliance; and

6. The establishment of additional program objectives and metrics, as required.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 14, 2016 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

---

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred twenty-five thousand dollars ($225,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Drew R. Slabaugh* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 414-5244 (704) 357-7914 – facsimile dslabaugh@serc1.org Gary Taylor* President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8205 (704) 357-7914 – facsimile gtaylor@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Anne Faugust* Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Leigh Anne Faugust
Counsel, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of 14 violations of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SERC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Risk	Penalty Amount
SERC2014014337	CIP-003-3	R4	Medium/ Severe	SR	Minimal	$180,000
SERC2014014336	CIP-003-3	R5	Lower/ Severe	SR	Minimal	
SERC2014014086	CIP-005-1	R1	Medium/ Severe	SR	Moderate	
SERC2014014427	CIP-005-3	R3	Medium/ Severe	SR	Moderate	
SERC2014014196	CIP-005-3a	R4	Medium/ Severe	SR	Minimal	
SERC2014013621	CIP-006-1	R1	Medium/ Severe	SR	Minimal	
SERC2014013444	CIP-006-3c	R1	Medium/ Severe	SC	Minimal	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Risk	Penalty Amount
SERC2014014195	CIP-006-1	R2	Medium/ Severe	SR	Minimal	$180,000
SERC2014014198	CIP-006-3c	R2	Medium/ Severe	SR	Moderate	
SERC2014013437	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014014395	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014013619	CIP-007-1	R5	Medium/ Severe	SR	Minimal	
SERC2014014423	CIP-007-1	R5	Lower/ Severe	SR	Minimal	
SERC2014014087	CIP-007-1	R6	Lower/ Severe	SR	Moderate	

SERC2014014337 CIP-003-3 R4 - OVERVIEW

SERC determined that URE did not fully implement its program to identify, classify, and protect information associated with Critical Cyber Assets (CCAs).

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE's failure to identify, classify, and protect CCA information repositories could allow unauthorized individuals access to CCA information. Nevertheless, although URE had not identified or maintained the CCA information repositories, its affiliate had identified the repositories and protected them as required. Personnel with access to the CCA information repositories were authorized. In addition, a malicious individual could not gain direct access to CCAs by gaining access to CCA information.

SERC determined the duration of the violation to be from the date URE incompletely implemented an update to its CIP compliance program, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review and document the URE repositories that contained CCA information;
2. ensure that access reviews for all repositories were reviewed under a compliance program;
3. complete the annual repository review;
4. research whether any additional repositories exist and add them to the repository list and perform the annual repository reviews as required; and
5. update policies/procedures to accept the lists and reviews done on repositories containing CCA information as part of the annual review to avoid duplication and relying on the existing access controls used for all repositories.

URE certified that it had completed its Mitigation Plan.

SERC2014014336 CIP-003-3 R5 - OVERVIEW

SERC determined that URE did not review at least annually the access privileges to protected CCA information in two instances. Failure of process ownership, human error, and employee turnover were the primary causes of this violation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to review the repositories annually could result in individuals having access to CCA information past the time such access is required. Such individuals could use CCA information to plan or coordinate attacks on CCAs. Nevertheless, URE regulates the access to the affected repositories based on physical and electronic access and grants access only to authorized personnel. URE has controls that remove physical and electronic access as part of its standard off-boarding procedure. URE would have removed access for any terminated individuals leaving during the time of the issue, minimizing the possibility of unauthorized personnel with access.

SERC determined the duration of the violation to be from the first day URE failed to complete the annual access review, through when URE completed its next annual access review.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. receive responses from repository owners regarding repository access;

2. update work level instructions regarding gathering and documenting responses that have been updated by the individuals who have been assigned to do that activity in order to meet current needs;
3. provide a notification email to the manager and individuals involved with the gathering of approvals for the annual review; and
4. test and update work-level instructions created for the missed review if required during the next review.

URE certified that it had completed its Mitigation Plan.

SERC2014014086 CIP-005-1 R1 - OVERVIEW

SERC determined that URE did not afford the protections of CIP-007 R1, R3, R4, R5, R6, and R8 to all Cyber Assets used in the Electronic Access Control and/or Monitoring (EACM) of the Electronic Security Perimeter (ESP) in seven instances. The instances were due to: 1) failures to follow documented procedures; 2) employee turnover; 3) inadequate transitioning of responsibilities; 4) failures to document changes adequately; 5) inadequate account review processes; 6) inadequate procedures; and 7) failure to notify asset owners.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to provide EACM devices the protective measures specified in CIP-007 R1, R3, R4, R5, R6, and R8 could leave EACM devices exposed to known vulnerabilities for an extended period. Nevertheless, several factors reduced the risk of the violation. For the CIP-007 R1 failure, URE authorized the changes that it did not properly document and implemented the changes using its documented change management procedure. For the CIP-007 R4 failure, URE had earlier versions of antivirus signatures running, providing protection against some viruses and malware. For the CIP-007 R5.1.3 failures, URE has controls that remove electronic access as part of its standard off-boarding procedure, and any terminated individuals leaving URE would have had their access revoked even if they still had an account on a specific EACM device not removed as required. For the CIP-007 R5.3.3 failures, URE determined that no one accessed the accounts in question after the passwords expired, and existing controls would force an individual trying to access the accounts to change the passwords. In addition, URE protected its EACM devices within Physical Security Perimeters (PSPs) and behind corporate firewalls that require two-factor authentication through a restricted VPN to access remotely.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review the active directory domain accounts to determine what accounts require a password reset, access removal, or Technical Feasibility Exception (TFE);
2. remove access to accounts deemed to no longer need their access either based on infrequent use or access of account determined to no longer be required;
3. reset the passwords on the accounts which still require access;
4. create a new process that will detect and change passwords automatically to ensure they do not exceed a year in time unless a TFE is required for the account;
5. document the new process as part of energy management and process control systems team's policies and procedures; and
6. communicate the policy/procedure change to the affected parties.

URE certified that it had completed its Mitigation Plan.

SERC2014014427 CIP-005-3 R3 - OVERVIEW

SERC determined that URE did not implement monitoring, logging, and alerting at all access points to the ESP 24 hours a day, seven days a week. The root cause of the violation was human error. Upon completion of a hardware replacement project, URE personnel reviewed firewall traffic to determine if URE was monitoring and logging all the Cyber Assets. However, URE should have reviewed the documented list of deployed Cyber Assets instead.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement logging or alerting at electronic access points to the ESP could result in unauthorized access and/or unauthorized access attempts going undetected. Nevertheless, URE had configured the devices to deny traffic by default and went through Cyber Vulnerability Assessments (CVAs) to validate that it had enabled only the ports and services required for operations.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify devices in scope;
2. verify devices are configured to send logs to the monitoring program;
3. verify monitoring program receives logs and maintains for 90 days;
4. develop a report that lists all devices that are logging and compare that against list of devices in inventory;
5. develop plan to implement a monitoring script that detects when logging fails for a device;
6. implement a monitoring script to ensure notification in the event monitoring fails;
7. implement a manual log review if logging/monitoring is unavailable;
8. validate that alerting rules are properly configured for affected devices; and
9. communicate and train on the new manual logging process.

URE certified that it had completed its Mitigation Plan.

SERC2014014196 CIP-005-3a R4 - OVERVIEW

SERC determined that URE did not document the execution status of its annual CVA action plans for electronic access points. SERC determined URE failed to include adequate procedures for ensuring its personnel updated the remediation action plans in a timely manner.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to take action on vulnerabilities identified during a CVA could allow malicious individuals to exploit known vulnerabilities in order to gain access to CCAs and other Cyber Assets. Nevertheless, the electronic access points (EAPs) at issue were virtual private networking devices utilized to secure communications between two remote locations, and did not allow direct access to CCAs. A PSP protected the EAPs.

SERC determined the duration of the violation to be from the date URE documented its action plans to remediate vulnerabilities identified in its CVA, through when URE updated the status of the CVA action plan for the open items.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the status column on the Mitigation Plan tab for all open items on the spreadsheet;
2. transition EAP assets to IT security who will track CVA statuses and remediation and update documentation;
3. follow IT security procedures that prescribe how CVA tracking and documentation is performed and how follow-up is to occur for the remediation action plan after it is created and initial contact with the asset owner is made;
4. show evidence of CVAs performed or timeline for performing CVAs on respective EAP assets; and
5. train on procedures that prescribe how CVA tracking and documentation is performed.

URE certified that it had completed its Mitigation Plan.

SERC2014013621 CIP-006-1 R1 - OVERVIEW

SERC determined that URE did not establish a completely enclosed (six-wall) border and it did not have alternative measures deployed nor documented at a PSP. URE discovered four holes in the back of a closet within a PSP. The openings within the closet would have led to an area designated as a non-PSP area. URE used a process to commission PSPs that was not robust and URE did not implement a rigorous process that required a thorough inspection of PSP boundaries.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that all Cyber Assets within an ESP reside completely within a six-wall border PSP could have allowed unauthorized individuals to gain physical access to CCAs. Nevertheless, the PSP is within a protected building secured by security cameras, contracted security personnel, and badge-access entry points, making it difficult for unauthorized individuals to gain access to the PSP. In addition, URE personnel staff the PSP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE sealed the four holes in the PSP.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. bolt the closet door shut;

2. update the PSP diagram to include the closet;
3. seal four holes by installing solid aluminum plating with screws from inside the PSP closet and with screws epoxied from outside the PSP;
4. inspect legacy sites;
5. perform an evaluation and complete repair of alarm on a door at a legacy site;
6. provide training to employees responsible for commissioning and PSP validation; and
7. update the checklists used for the PSP inspection process.

URE certified that it had completed its Mitigation Plan.

SERC2014013444 CIP-006-3c R1 - OVERVIEW

SERC determined that URE did not implement its documented visitor control program for continuous escort of visitors and logging visitor access to a PSP. The visitor was unescorted for approximately 15 minutes while repairing a printer and had not completed the necessary visitor access log.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to escort a visitor within a PSP and ensure that the visitor signed the visitor access log could have enabled the visitor to tamper with or physically damage CCAs without a record of them being in the PSP. Nevertheless, the visitor's access was limited to a room that did not contain CCAs. The CCAs were within an inner room and secured by additional doors that required badge access that the visitor did not possess. The visitor did not enter that room. In addition, URE personnel continually staffed the PSP containing the CCAs during the time that the visitor was unescorted.

SERC determined the duration of the violation to be from when the URE staff stopped escorting the visitor, through when the visitor left the PSP.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide coaching to the employee-contractor on visitor control;
2. implement physical security posters with security requirements and procedures; and
3. conduct staff meetings with the business units and review and reinforce the requirements of the CIP PSP visitor control program to continuously escort visitors and to have escorts require visitors to sign in and complete the visitor access log.

URE certified that it had completed its Mitigation Plan. SERC verified completion of URE's Mitigation Plan.

SERC2014014195 CIP-006-1 R2 - OVERVIEW

SERC determined that URE did not implement the operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week at three locations. The first location was an unsecured vent hatch; the second location was a small, energized space with a high risk of electrocution; and the third granted access to an airshaft. The root cause was insufficient training for personnel inspecting PSPs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to properly manage physical access at access points to the PSP using one of the access control methods authorized by CIP-006 R2 could allow unauthorized individuals to gain access to CCAs without being detected, allowing them to tamper with or destroy CCAs. Nevertheless, the access points at the first and third location were alarmed. The alarms would have alerted the appropriate monitoring workstation for a response in the event someone opened the access points—URE received no such alerts during the violation period. At the second location, an intruder would have gained access to a small space and risked electrocution to gain access to CCAs. In addition, the access points at the first and second locations were within secure facilities that URE personnel staffed and security guards monitored 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training to employees responsible for validating the PSP;
2. update the checklists used for the PSP inspection process;
3. permanently secure both sides of the metal bars to restrict access through the ventilation hatch at the third location;
4. install pad locks on all of the exterior doors at the second location;
5. put a roving patrol in place to ensure the doors in question were still locked and secured; and
6. install a hatch door at the first location.

URE certified that it had completed its Mitigation Plan.

SERC2014014198 CIP-006-3c R2 - OVERVIEW

SERC determined that URE did not afford the protective measures specified in CIP-007 R5.1.3 and R5.3.3 to Cyber Assets that authorize and/or log access to a PSP in two instances. The first instance was one user account on URE's Physical Access Control System (PACS) exceeded the annual password change requirement. The second instance was a failure to perform a first quarter review of authorized user accounts. The root cause was a failure to put controls in place to force password resets and premature implementation of controls that delayed an employee from having necessary access to generate the report for the first quarter review.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to change passwords on PACS on an annual basis and its failure to perform quarterly access reviews for PACS accounts could give malicious individuals additional time and opportunities to compromise PACS devices, allowing them to make unauthorized modification to physical access rights to CCAs. Nevertheless, access to the PACS requires either physical access, or logical access and two-factor authentication. No one had used the PACS account with the expired password in more than 120 days, which had caused the account to lock, requiring a password change upon the next login. A locked account requires administrator intervention after 120 days of inactivity, requiring a system administrator to reset the password. The account owner had a current personnel risk assessment (PRA) and attended the required cyber security training. For the user account review issue, URE has documented controls and procedures that remove physical and electronic access to Cyber Assets when appropriate, reducing the risk that an individual that should have been removed from the access list would retain the ability to access the PACS.

SERC determined the duration of the violation to be from the first day after the year in which URE did not change the PACS password, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. contact the account owner in order to work with the administrator to change the password;
2. transition support for device where the account with expired password resides;
3. create a new process that will detect and change passwords if an account has passed a pre-determined limit of days since the last password change;
4. document the change as part of policies and procedures; and
5. communicate the policy/procedure change to the affected parties.

URE certified that it had completed its Mitigation Plan.

SERC2014013437 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not immediately review and respond to a single unauthorized physical access attempt alarm in accordance with URE procedures during a 26-hour period when communications were down. The violation was due to a failure on the part of URE personnel to follow established procedures for notification.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to review and respond immediately to a received unauthorized access attempt alarm at one site during a 26-hour period when communications were down. Nevertheless, the card readers at the site continued to operate in a stand-alone mode during the loss of communications. All access and alarm activity cached at the card reader and downloaded to the server once the communication resumed. During this period, URE should have responded to one unauthorized access attempt alarm—URE handled the alarm appropriately after communication resumed. URE confirmed no individuals without authorization gained access to the site during this period. The site is protected by security fencing, security guards that monitor the site 24 hours a day, seven days a week, electronic access controls, and video cameras.

SERC determined the duration of the violation to be from when URE first lost communications with its alarm systems at one PSP, through when URE deployed security guards to monitor physical access to the PSP.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. issue an email to all supervisors and personnel providing details of the incident and the errors made;
2. issue disciplinary action notices to the three personnel and three shift supervisors who were involved in this incident;
3. develop a procedure for staff relief for the NERC regulated desk;
4. evaluate the training program, determine if any gaps exist, and develop a list of enhancements; and
5. update and perform the formal training program for relevant personnel.

URE certified that it had completed its Mitigation Plan.

SERC2014014395 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not implement controls to monitor access at all access points to the PSP. A remote facility experienced a loss of air conditioning and informed the command center that personnel would be propping open the door to maintain an acceptable temperature. A URE employee observed that the door to the PSP was propped open without a guard continuously monitoring the access point. The employee then notified security, which posted a guard at the access point.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor physical access to the PSP at issue could have allowed unauthorized individuals to gain physical access to and tamper with or destroy the CCAs inside. Nevertheless, URE deployed security guards on roving patrols that checked the PSP access point on an hourly basis starting when personnel first propped open the door. The guards continued the roving patrols until a guard posted to the PSP access point. The facility was located within a complex with personnel onsite 24 hours a day, seven days a week. In addition, a security fence with guards posted at the front gate secures the complex. Once URE identified the issue, a guard monitored the open door until the issue was resolved.

SERC determined the duration of the violation to be for approximately two and a half days when the PSP door was propped open without ensuring continuous monitoring.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. post a continuous monitoring guard at the propped open door until the door could be closed; and
2. send out an email to operations teams at the facility reminding them of the site-specific physical security plan that details the procedure for how to monitor propped open doors in a PSP.

URE certified that it had completed its Mitigation Plan.

SERC2014013619 CIP-007-1 R5 - OVERVIEW

SERC determined that URE did not annually change 11 account passwords associated with CCAs. URE had a technical password control deployed to force a password change after 365 days, but the control would only force a password change if there were an attempted login.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to change account passwords annually could leave Cyber Assets vulnerable to compromise through unauthorized use of an old password. Nevertheless, URE reviewed access logs and determined that no one had accessed the accounts in question since the date of password expiration. If an individual tried to access an account, the controls would have forced a password change. This issue affected two sites. PSPs and ESPs protected all affected Cyber Assets.

SERC determined the duration of the violation to be from the first day URE should have annually changed passwords, through when URE changed all passwords and filed a TFE for an account password that it could not change annually.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. expand password review to other registrations;
2. delete, disable, or change passwords on all of the affected accounts with one exception;
3. file a TFE for the one exception account;
4. review CVAs from its sites to assess its compliance with CIP-007-3c R5.3.3; and
5. develop preventive maintenance task to review password age of Cyber Assets.

URE certified that it had completed its Mitigation Plan. SERC verified completion of URE's Mitigation Plan.

SERC2014014423 CIP-007-1 R5 - OVERVIEW

SERC determined that URE did not document mitigating measures for Cyber Assets that could not technically enforce the password complexity requirement and did not submit a request for a TFE. The violation was limited to only one facility and was due to personnel failing to follow documented procedures to document compensating measures by filing for TFEs for Cyber Assets when appropriate.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its procedures to document compensating measures by filing a TFE when Cyber Assets were not technically capable of enforcing password complexity requirements increased the risk of unauthorized access to Cyber Assets within the ESP. Nevertheless, although it could not technically enforce the password complexity requirements on the Cyber Assets at issue, URE

checked the passwords and confirmed that they met the password complexity requirements, as required by its documented procedures. In addition, URE kept the Cyber Assets within a secure PSP and ESP, and all users had valid PRAs and cyber security training.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE filed its TFE with SERC.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to file a TFE for these devices for CIP-007-3 R5.3.

URE certified that it had completed its Mitigation Plan.

SERC2014014087 CIP-007-1 R6 - OVERVIEW

SERC determined that URE did not implement automated tools or organizational process controls to monitor system events related to cyber security. URE discovered that the centralized logging and monitoring system was not receiving cyber security events for CCAs. SERC determined the primary cause of the violation was the lack of procedural and technical controls to assess whether URE was monitoring cyber security events for all Cyber Assets within the ESP.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor system events related to cyber security for all Cyber Assets within the ESPs could have resulted in signs of a security breach going undetected. In addition, URE's failure to log system events related to security events could have impaired its ability to conduct an incident response. Nevertheless, this violation was limited to CCAs located at a single site. URE deployed an intrusion detection system to monitor the network on which the affected CCAs reside, and the CCAs resided within a PSP. URE did not discover or detect any cyber security events, Misoperations, or other adverse consequences because of the violation. Finally, URE could have reviewed the logs if an event occurred.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE corrected the settings on the domain-based firewall to allow the centralized logging and monitoring system to collect the event logs.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. remediate all devices by changing a configuration in a group policy;

2. update the CCA checklist to include steps to review logs manually in the event of a logging and monitoring device outage for any reason;
3. communicate the updated changes to the CCA checklist to the responsible individuals;
4. update the security status monitoring procedure;
5. communicate the updated changes to the security status monitoring procedure; and
6. perform a root cause analysis.

URE certified that it had completed its Mitigation Plan.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred eighty thousand dollars ($180,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC determined the compliance history should serve as an aggravating factor;
2. SERC considered certain elements of URE's internal compliance program (ICP) as a mitigating factor in the penalty determination. Specifically, URE's ICP is documented and readily available to its employees on its intranet. A URE compliance group reviews its ICP on an annual basis, which reports within URE's compliance department to ensure independence from the operations and engineering departments that must comply with the NERC Standards. URE employees receive quarterly newsletters to ensure awareness of ethics and compliance issues and annual CIP training. URE employees are also required to understand all corporate policies and procedures, including those related to compliance, and are subject to discipline, up to and including termination, for violating those policies. Nevertheless, SERC reduced ICP credit due to URE's compliance history and inability to prevent recurrence of CIP issues.
3. URE voluntarily self-reported 13 of the violations; five of the Self-Reports, however, came after notice of an upcoming Compliance Audit, and therefore did not receive mitigating credit;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. ten of these violations posed minimal risk and four violations posed moderate risk and did not pose a serious or substantial risk to the reliability of the BPS; and

7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred eighty thousand dollars ($180,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Prior to starting settlement discussions, SERC initiated meetings with URE compliance staff and middle management to discuss the high number of URE violations and the issues SERC was seeing with URE's compliance efforts. SERC management met with URE senior management after settlement discussions began to continue the discussion of SERC's concerns. To address SERC's concerns, URE met with SERC after reaching a settlement agreement to inform SERC of a comprehensive action plan that included the following elements:

1. The creation of an internal board, to ensure adequacy of cause and extent of condition analyses and review effectiveness of mitigation plans;

2. Enhanced oversight by an internal committee, along with enhanced reporting to provide members with immediate notification of possible violations;

3. Enhanced mitigation plan tracking at the enterprise level to allow for regular status reporting;

4. Quarterly meetings with SERC to discuss progress and solicit feedback;

5. The review and enhancement of URE's communication plan to educate business continually on the company's approach to ensure NERC compliance; and

6. The establishment of additional program objectives and metrics, as required.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 14, 2016 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Drew R. Slabaugh* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 414-5244 (704) 357-7914 – facsimile dslabaugh@serc1.org Gary Taylor* President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8205 (704) 357-7914 – facsimile gtaylor@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Faugust* Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Leigh Faugust
Counsel, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

October 31, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of 19 violations of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of one million one hundred twenty-five thousand dollars ($1,125,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC2014014352	CIP-002-3	R3	High/Severe	SR	Serious	$1.125M
WECC2014013782	CIP-003-3	R6	Lower/ Severe	SR		
WECC2014014353	CIP-005-3a	R1	Medium/ Severe	SR		
WECC2014013507	CIP-005-3a	R2	Medium/ Severe	SC		
WECC2014013783	CIP-005-3a	R3	Medium/ Severe	SR		
WECC2014014354	CIP-005-3a	R4	Medium/ Severe	SR		
WECC2014014355	CIP-005-3a	R5	Lower/ Severe	SR		

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC2014014356	CIP-006-3c	R1	Medium/ Severe	SR		
WECC2014014357	CIP-006-3c	R2	Medium/ Severe	SR		
WECC2014014358	CIP-006-3c	R3	Medium/ Severe	SR		
WECC2014013785	CIP-006-3c	R4	Medium/ Severe	SR		
WECC2014013784	CIP-006-3c	R5	Medium/ Severe	SR		
WECC2014014359	CIP-006-3c	R6	Lower/ Severe	SR		
WECC2014014360	CIP-007-3a	R1	Medium/ Severe	SR		
WECC2014014361	CIP-007-3a	R2	Medium/ Severe	SR		
WECC2014014362	CIP-007-3a	R3	Lower/ Severe	SR		
WECC2014014363	CIP-007-3a	R5	Lower/ Severe	SR		
WECC2014014364	CIP-007-3a	R6	Lower/ Severe	SR		
WECC2014014365	CIP-007-3a	R8	Lower/ Severe	SR		

ROOT CAUSES FOR VIOLATIONS

The root cause of the violations was URE's failure to have a comprehensive change management, configuration, and communication process during the project, testing, and installation phases of new substations. Further, URE failed to have a change management process that included verification that

NERC CIP Standards had been implemented. Specifically, URE's change management process for commissioning new Critical Asset substations did not specifically require the individual steps necessary to ensure that new Critical Assets be afforded all the electronic and physical controls necessitated by NERC CIP Standards. The change management process did not include requirements for testing and verification of CIP protections. URE's change management did not include an independent inspection of the installation of Critical Cyber Assets (CCAs), Electronic Access Control and Monitoring devices (EACMs), and Physical Access Control Systems (PACS).

Additional causes for the violations include the following failures or omissions:

1. Personnel responsible for constructing the new facilities were aware that the new facilities were required to have CIP protections, and those personnel were trained in the CIP Standards. Training related to the change control procedures and the URE internal compliance program (ICP) provided to those personnel was ineffective;
2. Construction personnel did not have well-defined responsibility and accountability for ensuring those facilities were compliant with NERC CIP Standards. Accountability placed with these individuals could have reduced the likelihood of the violations from occurring;
3. URE personnel failed to follow defined URE policies and procedures requiring that CCAs associated with Critical Assets are included in an inclusive inventory of CCAs. Such identification could have helped prevent the violations from occurring;
4. URE's processes required construction personnel to work with information technology personnel to ensure logical protections were in place. Nevertheless, communication between these groups failed, and the work required was not coordinated between the groups;
5. URE lacked adequate supervision over monitoring the status of the project progress in that NERC CIP compliance should have been included within the scope of the project, which could have prevented the violations from occurring; and
6. URE failed to consider industry observations from other entities' experience with building Critical Asset substations, which could have improved URE's change management process and potentially prevented the violations.

AGGREGATE RISK TO THE BULK POWER SYSTEM (BPS) FROM VIOLATIONS

URE connected substations to the Bulk Electric System (BES) without ensuring those substations were afforded adequate CIP protections to electronically and physically protect the CCAs contained therein, prior to being energized and activated. Specifically, URE failed to protect the substations with firewalls, as well as failed to complete its physical access control system configurations. Numerous consequences could follow the failure to ensure CIP protections to electronically and physically protect the aforementioned CCAs prior to energizing the substations. For example, there was an increased risk that a malicious individual would enter the substation without a key, badge, or authorization and take

any number of negative actions. The malicious individual could have physically destroyed CCAs within the substations, or could have modified relay settings to prevent relays from opening upon a detected fault in the line, allowing the fault to continue and potentially damage neighboring substations.

URE did have controls in place to mitigate the risk of cyber and physical attacks on the substation. Specifically, URE implemented some electronic and physical controls as part of a defense-in-depth architecture, such as the substations' systems use of standardized hardened operating systems, anti-malware (where technically feasible), security event logging, and account management. Additionally, the substations' wide-area and local-area electric operations industrial control systems networks are private and segmented from URE corporate networks electric operations. The routers at the substations controlled local network access through policies on the routers. The substations' BES systems used active directory groups and terminal access controller access control systems to control and monitor users' interactive electronic access. As preventive controls, the substations also had fences, locks, access authorizations, a visitor control program, and physical security programs in place—despite not having an established and adequate Physical Security Perimeter (PSP). Notwithstanding URE's controls, it failed to provide the adequate CIP protections for these substations for a substantial period.

WECC considered the risk posed by these violations to the reliability of the BPS and determined that these violations collectively posed a serious and substantial risk to the reliability of the BPS.

WECC2014014352 CIP-002-3 R3 - OVERVIEW

WECC determined that URE failed to update its CCAs list during the calendar year.

WECC determined the duration of the violation to be from the date when URE energized the first substation without updating its list of CCAs, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Assess and identify all procedures associated with the Critical Asset identification process procedure;
2. Ensure that the Critical Asset identification procedure is properly integrated and referenced in significant phases (e.g., study construction planning, construction, release to operations, etc.); and
3. Integrate compliance verification procedures and require CIP senior manager sign-off prior to release to operations.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013782 CIP-003-3 R6 - OVERVIEW

WECC determined that URE failed to utilize its process of change control and configuration management for adding, modifying, replacing, or removing CCAs, as well as EACMs and PACS hardware or software. Additionally, URE failed to implement supporting configuration management activities to identify, control, and document all changes pursuant to the change control process.

WECC determined the duration of the violation to be from the date when URE energized the first substation without following change control and configuration management processes, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Modify URE's internal process walk-down checklist to include CIP assessment;
2. Implement tailboards and training within 30 days of the release of the modified URE's internal process walk-down checklist;
3. Review the electric system engineering manual process book to determine inclusion points for CIP assessment process;
4. Implement a new process that contains a release to operations checklist;
5. Implement an enterprise compliance tracking system compliance task for the CIP-002-3 standard lead to perform an annual review of the electric transmission project portfolio in order to identify potential incoming CIP applicable projects;
6. Modify URE's internal process to include comprehensive documentation which includes assessments and the CIP implementation requirements for all CIP standards in order to be given to the project engineer;
7. Implement tailboards and training within 30 days of the release of the modified URE internal process;
8. Update the electric system engineering manual process book with CIP assessment process and references to corporate CIP standards;
9. Review and perform a quality assurance table top test of the processes to ensure communication, implementation, and sign-off; and
10. Provide tailboard and training on the modified electric system engineering manual process book with new CIP assessment references and corporate CIP standards.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014353 CIP-005-3a R1 - OVERVIEW

WECC determined that URE failed to ensure that CCAs resided within an Electronic Security Perimeter (ESP), as well as to identify and document the ESP and all access points to the perimeter.

WECC determined the duration of the violation to be from when URE energized the first substation without ensuring the ESP and all access points were appropriately protected, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Apply protective measures including access control through monitoring electronic access into ESP; and
3. Update the CIP Cyber Asset inventory list.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013507 CIP-005-3a R2 - OVERVIEW

WECC determined that URE failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all Electronic Access Points to the ESP.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing electronic access controls, through when URE activated its firewall and applied the appropriate ESP CIP protections to the CCAs at the substations.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Modify IT project management documents to ensure that all IT projects identify potential CIP requirements at project initiation and that all applicable CIP requirements are completed and validated prior to project completion;
2. Train infrastructure project managers on the modified processes and procedures;

3. Finalize, approve, and publish all new and modified documentation associated with this Mitigation Plan; and
4. Review and approve certification of plan and evidence.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013783 CIP-005-3a R3 - OVERVIEW

WECC determined that URE failed to implement and document electronic or manual processes for monitoring and logging access at ESP access points.

WECC determined the duration of the violation to be from when URE energized the first substation without monitoring or logging electronic access, through when URE activated its firewall and applied the appropriate ESP CIP protections to the CCAs at the substations.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Modify IT project management documents to ensure that all IT projects identify potential CIP requirements at project initiation and that all applicable CIP requirements are completed and validated prior to project completion;
2. Train infrastructure project managers on the modified processes and procedures;
3. Finalize, approve, and publish all new and modified documentation associated with this Mitigation Plan; and
4. Review and approve certification of plan and evidence.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014354 CIP-005-3a R4 - OVERVIEW

WECC determined that URE failed to perform a Cyber Vulnerability Assessment (CVA) of the Electronic Access Points to the ESPs at least annually.

WECC determined the duration of the violation to be from when URE energized the first substation without including the access points in its CVA, through when URE included all EACM devices for the established ESPs in its CVA.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish ESPs at both substations by installing and configuring the firewalls;
2. Apply protective measures including access control monitoring of electronic access into an ESP;
3. Update the CIP Cyber Asset inventory list; and
4. Include all EACMs for the established ESPs for the annually scheduled CVA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014355 CIP-005-3a R5 - OVERVIEW

WECC determined that URE failed to: 1) ensure that all documentation reflected current configurations and process; 2) update documentation to reflect the modification of the network or controls within ninety calendar days of the change; and 3) retain electronic access logs for at least 90 calendar days.

WECC determined the duration of the violation to be from when URE failed to review, update, and maintain its CIP-005 documentation, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Create a new ESP drawing for its substations, to be reviewed annually;
2. Establish the ESPs at its substations by installing and configuring the firewalls; and
3. Update the CIP Cyber Asset inventory list.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014356 CIP-006-3c R1 - OVERVIEW

WECC determined that URE failed to document, implement, and maintain a physical security plan.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing a physical security plan, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to complete installation of PSP physical security controls for its substations.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014357 CIP-006-3c R2 - OVERVIEW

WECC determined that URE failed to ensure that all PACS were afforded required protective measures.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing protections to the PACS, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Modify IT project management documents to ensure that all IT projects identify potential CIP requirements at project initiation and that all applicable CIP requirements are completed and validated prior to project completion;
2. Train infrastructure project managers on the modified processes and procedures;
3. Finalize, approve, and publish all new and modified documentation associated with this Mitigation Plan; and
4. Review and approve certification of plan and evidence.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014358 CIP-006-3c R3 - OVERVIEW

WECC determined that URE failed to ensure that Cyber Assets used in the access control and/or monitoring of the ESP resided within an identified PSP.

WECC determined the duration of the violation to be from when URE energized the first substation without ensuring that EACM devices were enclosed within a PSP, through when URE established a PSP at the substations.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESP at its substations by installing and configuring the firewalls;
2. Complete installation of PSP physical security controls, protecting the EACMs, in the substations; and
3. Update the CIP Cyber Asset inventory list with the EACMs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013785 CIP-006-3c R4 - OVERVIEW

WECC determined that URE failed to document and implement operational and procedural controls to manage physical access at all access points to the PSP 24 hours a day, seven days a week.

WECC determined the duration of the violation to be from when URE energized the first substation without providing physical access controls, through when URE established a PSP at the substations.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Complete the installation of PSP physical security controls in its substations; and
2. Create an attestation of PSP commissioning and required criteria needed before a Cyber Asset is declared operational or changed.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013784 CIP-006-3c R5 - OVERVIEW

WECC determined that URE failed to document and implement the technical and procedural controls for monitoring physical access at all access points to all PSPs 24 hours a day, seven days a week, and failed to immediately review and handle all unauthorized access attempts.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing physical access monitoring, through when URE established a PSP at the substations.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Complete the installation of PSP physical security controls in its substations; and
2. Create an attestation of PSP commissioning and required criteria needed before a Critical Asset is declared operational or changed.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014359 CIP-006-3c R6 - OVERVIEW

WECC determined that URE failed to log physical access with sufficient information to identify individuals uniquely and the time of access 24 hours a day, seven days a week. WECC determined that URE also failed to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSP using computer logging, video recording, or manual logging.

WECC determined the duration of the violation to be from when URE energized the first substation without establishing the appropriate physical entry logging at all access points to the PSP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to complete the installation of PSP physical security controls in its substations.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014360 CIP-007-3a R1 - OVERVIEW

WECC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls.

WECC determined the duration of the violation to be from when URE energized the first substation without ensuring that new Cyber Assets did not adversely affect existing cyber security controls, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Update the CIP Cyber Asset inventory list; and
3. Apply testing procedures to the new Cyber Assets within the established ESP.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014361 CIP-007-3a R2 - OVERVIEW

WECC determined that URE failed to establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations were enabled.

WECC determined the duration of the violation to be from when URE energized the first substation without ensuring that only those ports and services required for normal and emergency operations were enabled, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Update the CIP Cyber Asset inventory list; and
3. Update the Cyber Asset whitelist (ports and services) to include the new Cyber Assets within the established ESPs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014362 CIP-007-3a R3 - OVERVIEW

WECC determined that URE failed to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing a security patch management program, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Update the CIP Cyber Asset inventory list; and
3. Update the security patches, where technically feasible, to the new Cyber Assets within the established ESPs, including PACS.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014363 CIP-007-3a R5 - OVERVIEW

WECC determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

WECC determined the duration of the violation to be from when URE energized the first substation without implementing account management activities, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Update the CIP Cyber Asset inventory list; and
3. Apply authentication and access control for individual and shared accounts, and maintain user activity logs for the Cyber Assets within the established ESPs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014364 CIP-007-3a R6 - OVERVIEW

WECC determined that URE failed to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events related to cyber security.

WECC determined the duration of the violation to be from when URE energized the first substation without ensuring security status monitoring, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Establish the ESPs at its substations by installing and configuring the firewalls;
2. Update the CIP Cyber Asset inventory list; and
3. Apply security monitoring, where technically feasible, to the Cyber Assets within the established ESPs.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014014365 CIP-007-3a R8 - OVERVIEW

WECC determined that URE failed to perform a CVA of all Cyber Assets within the ESP annually.

WECC determined the duration of the violation to be from when URE energized the first substation without completing a CVA, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Update the CIP Cyber Asset inventory list; and
2. Ensure that the current CIP Cyber Asset inventory list is used for the annually scheduled CVA.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one million one hundred twenty-five thousand dollars ($1,125,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC determined the compliance history should serve as an aggravating factor;
2. WECC did not consider URE's ICP as a mitigating factor in the penalty determination because of the ICP's significant failure in this case;
3. URE self-reported 18 of the violations after consultation with WECC about a self-certified noncompliance, resulting in minimal credit;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. Considered in the aggregate, the 19 violations posed a serious and substantial risk to the reliability of the BPS;
7. URE is developing and implementing a project to improve the work management process by replacing the multiple systems and tools previously used with a single unified system applied across the URE enterprise. The project will significantly improve the reliability and security of URE's system and help URE avoid noncompliance with these standards in the future. Specifically, the improvement in work management processes, as well as the improved controls, timeliness, and quality for asset data quality will significantly reduce the risk of potential security and compliance events caused by an inaccurate inventory of BES Cyber

Systems and their associated assets. The project goes above and beyond meeting the minimum NERC CIP requirements by providing best practices to ensure that NERC CIP compliance is met and maintained on an ongoing basis with minimal errors given the automation in the system; and

8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one million one hundred twenty-five thousand dollars ($1,125,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one million one hundred twenty-five thousand dollars ($1,125,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel, Corporate Secretary Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

October 31, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of four violations of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to other remedies

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC2014013506	CIP-002-3	R4	Lower/ Moderate	SC	Moderate	$250,000
WECC2014013873	CIP-005-3a	R1	Medium/ Severe	SR		
WECC2014014531	CIP-006-3c	R2		SR		
WECC2015014704	CIP-007-3a	R8		SC		

WECC2014013506 CIP-002-3 R4 - OVERVIEW

WECC determined that URE failed to approve its Critical Cyber Assets (CCAs) list during one calendar year. WECC also determined that URE completed its annual inventory, but that the CIP senior manager failed to review and approve the list within the required timeframe.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). An inaccurate list of CCAs could potentially leave Cyber Assets that are essential to the operation of an identified CCA unknown and unprotected. Failing to protect these essential Cyber Assets could lead to misuse or compromise of the Cyber Asset, leading to

a negative impact on the associated CCA. While URE implemented alternative controls to prevent unauthorized access to CCAs, including a seven-step process for updating the CCA list and ongoing updates through the change control process, URE's measures failed in this instance. URE did not discover that it had failed to approve its CCA list until URE was preparing for its Self-Certification submittal. Nevertheless, URE completed the annual inventory on time and submitted it to the CIP senior manager for approval. The CIP senior manager failed to complete this task within the required period.

WECC determined the duration of the violation to be the entire calendar year for the certain missed compliance period.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Perform a process review to identify and clarify the communication and work flow requirements;
2. Test the process to ensure the work flow and communication requirements;
3. Draft and implement an automated task to meet the process requirements; and
4. Test and validate the automated task notification and functionality.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2014013873 CIP-005-3a R1 - OVERVIEW

WECC determined that URE failed to identify and document all access points to the Electronic Security Perimeter (ESP). WECC determined that URE failed to provide an access point all the required protective measures and failed to maintain documentation of all electronic access points to the ESP.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE connected one switch in the test environment to the control center ESP, creating an undocumented access point into that ESP. Failing to identify an ESP access point and afford it with CIP protections could allow a malicious person to discover the access point by scanning URE or by gaining physical access to the device. The malicious person could then launch a malware attack on the switch to attempt to gain logical access to the device. If the attack were successful, the malicious person could then use the device to send attack packets into the ESP, which houses the Supervisory Control and Data Acquisition (SCADA), Energy Management System, and Remedial Action Scheme system, and potentially gain control of one of those systems, thereby compromising up to five pieces of Bulk Electric System (BES) equipment. Additionally, the device was part of a test network. If

vulnerabilities are introduced into the test network, the vulnerabilities could spread from the test environment to the control center ESP.

Nevertheless, URE implemented both preventive and detective controls. As preventive controls, the switch was located inside an area that requires key card access, and URE uses anti-virus software in the ESP to monitor traffic. As additional preventive measures, URE uses an intrusion prevention system, which also monitors traffic for malware and could stop a malware attack. Further, the applicable devices were contained in a secure and locked facility only accessible by SCADA technicians who all have NERC CIP logical and physical access. As detective measures, URE has personnel in the control center around the clock, who would detect any change in generation. In addition, URE uses event logging and monitoring of devices in the ESP, which could have detected repeated access attempts.

WECC determined the duration of the violation to be from when URE installed the switch connecting the test environment and control center through when URE removed the switch from the ESP.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Evaluate existing processes using lessons learned from this instance, and others, to determine if there are sections that need to be strengthened or added;
2. Implement and operationalize any design modifications identified above, including workforce training;
3. Implement technology and procedures to continuously baseline assets located within ESP and detect deltas due to changes, strengthening design of the control;
4. Identify and implement a process to evaluate the effectiveness of the training of all personnel performing work within these environments, strengthening operation of the control;
5. Observe performance and collect evidence for a 90-day period to ensure its effectiveness prior to closing out the Mitigation Plan;
6. Implement CIP Version 5 procedure for ports and service procedure, change management procedure, and signage controls on BES Cyber Assets;
7. Implement the change management procedure and track controls to trigger updates to inventory list and ESP drawings;
8. Implement CIP Version 5 procedure for operationalizing the new signage controls on BES Cyber Assets;
9. Operationalize the signage controls on BES Cyber Assets;
10. Operationalize the change management procedure into work processes;
11. Evaluate effectiveness of signage controls on BES Cyber Assets;
12. Evaluate effectiveness of change management procedure controls for updating inventory list and ESP drawings; and

13. Modify, if necessary, and re-publish ports and services procedures and change management procedures.

WECC2014014531 CIP-006-3c R2 - OVERVIEW

WECC determined that URE failed to ensure that its Cyber Assets that authorize and/or log access to the Physical Security Perimeters (PSPs) be afforded the protective measures specified in CIP-006-3c.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Software was implemented on URE's Physical Access Control System (PACS) servers; anyone with the appropriate access to this software could grant and revoke access to all of URE's PSPs. As a result, a larger number of personnel had the ability to provision access to PSPs. This could allow a malicious, unauthorized individual to provision unauthorized personnel into any PSP. Once access was granted, the unauthorized individual could physically destroy or harm CCAs, attempt to logically access devices and modify configurations, or input a virus with a universal serial bus (USB) device. These CCAs were in this increased vulnerable state for an extended period.

Nevertheless, URE implemented preventive and detective controls. Specifically, URE's primary and back-up control centers are staffed around the clock, thereby reducing the likelihood of malicious personnel destroying or manipulating CCAs. Additionally, URE implemented strong username and password login restrictions to all CCAs, thereby reducing the likelihood of malicious personnel gaining unauthorized electronic access to these devices. In addition, URE uses a corporate-wide anti-virus solution to prevent the introduction and spread of a virus implanted with a USB device. As a corrective control, URE implemented backups of its servers so they could be restored to a trusted state.

WECC determined the duration of the violation to be from when URE implemented a certain software that began provisioning access to the PSPs without the required protections through when URE enhanced the specific software's functionality and security with the required protections.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Demonstrate compliance of system security to meet best business practice and CIP compliance; and
2. Qualify scope of PACS categorization relative to NERC CIP Version 5.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC2015014704 CIP-007-3a R8 - OVERVIEW

WECC determined that URE failed to perform a Cyber Vulnerability Assessment (CVA) of all Cyber Assets within the ESP at least annually.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE failed to perform a CVA of all Cyber Assets within the ESP. Specifically, URE would sample like devices while performing the CVA and would not perform a CVA of all applicable devices. Failure to conduct a CVA could allow cyber vulnerabilities to go undetected, potentially allowing for exploitation by a malicious person to launch cyber-attacks against CCAs essential to the operation of BES.

URE implemented both preventive and detective controls. As preventive controls, URE's network employs defense in depth that monitors incoming traffic to the network. URE's firewalls use access control lists to permit only traffic from known IP addresses, denying all other traffic. The firewalls also require multi-factor authentication for remote users. URE also uses electronic and physical access controls, requiring PINs and access cards in order to gain access into the PSPs containing CCAs. If access to the PSP were obtained by a malicious person, URE utilizes around-the-clock security personnel. As detective controls, URE uses logging on its devices, including firewalls, to alert unauthorized access attempts. In addition, URE uses alarms to alert for changes in load and URE did perform a CVA on some assets, but not for all required assets.

WECC determined the duration of the violation to be from the beginning of the calendar year in which URE first failed to complete a CVA through the end of the last year when URE completed a CVA that did not include all Cyber Assets.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Determine involvement of other processes and procedures;
2. Develop process flow to reflect new CIP standard and links to other identified processes and procedures;
3. Complete a CVA for the previous calendar year to include previously missed Cyber Assets residing within established ESPs;
4. Revise the procedure to reflect lessons learned and feedback from stakeholders, as well as the new CIP Version 5 vulnerability assessment requirements;
5. Pilot the new process;
6. Modify the process and procedures; and
7. Approve and published processes and procedures as appropriate.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's CIP compliance history to be an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations which WECC considered a mitigating factor;
3. URE voluntarily self-reported two of the violations; however, URE did not receive mitigating credit for one of the violations because the Self-Report was submitted during the Self-Certification period;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. all four violations posed a moderate risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred fifty thousand dollars ($250,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred fifty thousand dollars ($250,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel, Corporate Secretary Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

November 30, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[2] discussed in detail in the Notice of Confirmed Violation (NOCV), in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

NERC is filing this Notice of Penalty with the Commission because Midwest Reliability Organization (MRO) has issued an NOCV to resolve all outstanding issues arising from MRO's determination and findings of three violations of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

NERC is filing this Notice of Penalty with the Commission because, based on information from MRO, URE does not dispute the violations and the one hundred forty-two thousand dollar ($142,000) penalty assessed to URE.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the NOCV issued by MRO. The details of the findings and basis for the penalty are set forth in the NOCV and herein. This Notice of Penalty filing contains the basis for approval of the NOCV by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV. Further information on the subject violations is set forth in the NOCV and herein.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
MRO2015014792	CIP-002-3	R3	High/ Severe	CA	Moderate	$142,000
MRO2015014793	CIP-005-1	R1	Medium/ Severe			
MRO2015014794	CIP-007-1	R1.1 R1.3				

MRO2015014792 CIP-002-3 R3 - OVERVIEW

MRO determined that URE did not develop a complete list of all the required Critical Cyber Assets (CCAs). Specifically, URE did not list certain Inter-Control Center Communications Protocol (ICCP) servers as CCAs. The cause of this violation was URE's reliance upon a third-party vendor that incorrectly advised URE that locating the ICCP servers outside of the Electronic Security Perimeter (ESP) was prudent and would improve security.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, the ICCP servers were essential to the operation of the primary and backup control centers. URE used them to exchange real-time information for

essential functions including: generator set point values; Special Protection System status; breaker status; and megawatt line flows between URE and its Reliability Coordinator. If the generator set point data is not available to the URE control center or the URE supervisory control and data acquisition (SCADA) data is not available to its Reliability Coordinator, there could be an adverse effect on the reliable operation of the BPS.

Nevertheless, while URE did not classify the ICCP servers as CCAs, it was protecting the servers as if they were CCAs. Specifically: 1) the servers were located inside of a Physical Security Perimeter (PSP), and any individuals with logical or physical access had each undergone a background check; 2) any significant change to the servers met the requirements of URE's change control and configuration management program; 3) URE patched the servers and evaluated all applicable security patches monthly; 4) URE utilized account management techniques including password complexity and logging measures to reduce the risk of intrusion by an adversary; and 5) URE documented all active and enabled ports and services and utilized a program to monitor for unauthorized usage.

Finally, MRO reviewed network architecture. URE used firewalls to block and limit unwanted external network traffic from entering both the ICCP servers and the ESP. This reduced the potential amount of untrusted network traffic from accessing the ICCP servers and ESP. During the network review, MRO ascertained that the ICCP servers were behind a corporate firewall, yet not in a defined ESP where CCAs are required to be located. The ICCP servers were logically isolated from the ESP per vendor recommendation.

MRO determined the duration of the violation was from when URE activated the ICCP servers that were not listed as CCAs through Mitigation Plan completion.

To mitigate this violation, URE:

1. implemented new ESPs at the primary control center and at the backup control center;
2. moved the ICCP server nodes to logically migrate the ICCP servers to new segments off the control center firewalls and declared these networks as ESPs; and
3. created and implemented new Cyber Asset procedures to ensure that new devices added to an ESP are compliant with the NERC Reliability Standards.

MRO verified that URE completed all mitigation activities.

MRO2015014793 CIP-005-1 R1 - OVERVIEW

MRO determined that URE failed to meet the requirements of CIP-007-1 (test procedures) for a Cyber Asset used in the access control and monitoring of the ESP. Specifically, sampling revealed that a CCA, an Electronic Access Control and Monitoring (EACM) device, underwent a significant change, and the requisite test procedures associated with that significant change were not adequately documented. The URE procedure was incomplete and did not list the performance test steps, which led to the failure to produce sufficient evidence to demonstrate that testing was performed, the specific test steps to be performed, and the test procedures.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE performed some testing for adverse impacts to user security controls; however, it did not document all required testing. Through discussion with the URE subject matter expert, it was determined that the change made to the CCA was intended to be tracked in the security testing spreadsheet; however, the actual testing performed was not documented.

After discussions with the URE subject matter expert, MRO ascertained that URE completed user account reviews for default and administrator accounts, but not individual named user accounts.

Moreover, URE was performing other CIP user security requirements. Specifically, URE implemented technical and procedural controls to manage authentication and authorization, including tracking user access and managing password complexity rules for monitoring devices. MRO did not discover any noncompliance where URE did not perform periodic user account reviews for monitoring devices. MRO did not discover any noncompliance in situations where Cyber Assets within the ESP did not have technically feasible, automated tools or organizational process controls to monitor system events related to cyber security. Finally, MRO did not discover any noncompliance related to performing logging and managing log retention for monitoring devices.

MRO determined the duration of the violation was from when the standard became mandatory and enforceable on URE through Mitigation Plan completion.

To mitigate this violation, URE:

1. upgraded the testing software used for the devices to incorporate the Tripwire policy module for the numerous high impact Bulk Electric System (BES) Cyber Assets;
2. retired the spreadsheet legacy checklist procedure and developed and implemented new procedures; and
3. trained staff on new procedures.

MRO verified that URE completed all mitigation activities.

MRO2015014794 CIP-007-1 R1.1 & R1.3 - OVERVIEW

MRO determined that URE failed to document its testing process sufficiently to include detailed steps for account testing and to document the associated test results sufficiently. Specifically, sampling revealed that a CCA, an EACM device, underwent a significant change, and the requisite test procedures associated with that significant change were not adequately documented. The URE procedure was incomplete and did not list the performance test steps, which led to the failure to produce sufficient evidence to demonstrate that testing was performed, the specific test steps to be performed, and the test procedures.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE performed some testing for adverse impacts to user security controls; however, it did not document all required testing. Through discussion with the URE subject matter expert, it was determined that the change made to the CCA was intended to be tracked in the security testing spreadsheet, however, the actual testing performed was not documented. After discussions with the URE subject matter expert, MRO ascertained that URE completed user account reviews for default and admin accounts, but not individual named user accounts.

Nevertheless, URE was performing other CIP user security requirements. Specifically, URE implemented technical and procedural controls to manage authentication and authorization, including tracking user access and managing password complexity rules for monitoring devices. MRO did not discover any noncompliance where URE did not perform periodic user account reviews for monitoring devices. MRO did not discover any noncompliance in situations where Cyber Assets within the ESP did not have technically feasible, automated tools or organizational process controls to monitor system events related to cyber security. Finally, MRO did not discover any noncompliance related to performing logging and managing log retention for monitoring devices.

MRO determined the duration of the violation was from when the standard became mandatory and enforceable on URE through Mitigation Plan completion.

To mitigate this violation, URE:

1. upgraded the testing software used for the devices to incorporate the Tripwire policy module for the numerous high impact BES Cyber Assets;

2. retired the spreadsheet legacy checklist procedure and developed and implemented new procedures; and
3. trained staff on new procedures.

MRO verified that URE completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Notice of Confirmed Violation, MRO has assessed a penalty of one hundred forty-two thousand dollars ($142,000) for the referenced violations. In reaching this determination, MRO considered the following factors:

1. MRO considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which MRO considered a neutral factor;
3. MRO did not consider URE's initial level of cooperation to be a mitigating factor in the initial penalty determination. Following a post-audit meeting with URE representatives, MRO noticed a significant change in the level of cooperation during the development and implementation of mitigation. MRO considered the involvement of senior management in the process as evidence of a strong commitment to the security and reliability of the BPS. Thereafter, MRO considered URE's cooperation to be a mitigating factor in the penalty determination;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations posed a moderate and not serious or substantial risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, MRO determined that, in this instance, the penalty amount of one hundred forty-two thousand dollars ($142,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the NOCV and supporting documentation on October 31, 2016 and approved the NOCV. In approving the NOCV, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the NOCV and believes that the assessed penalty of one hundred forty-two thousand dollars ($142,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Daniel P. Skaar* President Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1731 dp.skaar@midwestreliability.org Sara E. Patrick* Vice President of Compliance Monitoring and Regulatory Affairs Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1708 se.patrick@midwestreliability.org Jackson Evans* Enforcement Attorney Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1758 jj.evans@midwestreliability.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Anne Faugust* Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Leigh Anne Faugust
Counsel, Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
Midwest Reliability Organization

December 29, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of 31 violations of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement and herein.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC201002377	CIP-003-1	R5	Lower/ Severe	GO, GOP	SC	Moderate	No Penalty
WECC201002208	CIP-004-1	R2	Medium/ Severe		SC	Moderate	
WECC201002209	CIP-004-1	R3	Medium/ Severe		SC	Moderate	
WECC201002210	CIP-004-1	R4	Medium/ Severe		SC	Moderate	
WECC2015014575	CIP-004-3	R2	Lower/ Severe		SR	Moderate	
WECC201002218	CIP-005-1	R1	Lower/ Severe		SC	Moderate	
WECC201002219	CIP-005-1	R2	Lower/ Severe		SC	Moderate	
WECC201002220	CIP-005-1	R3	Medium/ Severe		SC	Moderate	
WECC201002221	CIP-005-1	R4	Lower/ Severe		SC	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC201002222	CIP-005-1	R5	Medium/ Severe	GO, GOP	SC	Minimal	No Penalty
WECC201002167	CIP-006-1	R2	Medium/ Severe		SC	Moderate	
WECC201002205	CIP-006-1	R3	Medium/ Severe		SC	Moderate	
WECC201002206	CIP-006-1	R4	Lower/ Severe		SC	Moderate	
WECC201002207	CIP-006-1	R5	Lower/ Severe		SC	Minimal	
WECC201002211	CIP-006-1	R6	Medium/ Severe		SC	Moderate	
WECC201002168	CIP-007-1	R1	Medium/ Severe		SC	Moderate	
WECC201002204	CIP-007-1	R2	Medium/ Severe		SC	Moderate	
WECC201002212	CIP-007-1	R3	Lower/ Severe		SC	Moderate	
WECC201002223	CIP-007-1	R4	Medium/ Severe		SC	Moderate	
WECC201002224	CIP-007-1	R5	Medium/ Severe		SC	Moderate	
WECC201002225	CIP-007-1	R6	Medium/ Severe		SC	Moderate	
WECC201002226	CIP-007-1	R7	Lower/ Severe		SC	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC201002227	CIP-007-1	R8	Medium/ Severe	GO, GOP	SC	Moderate	No Penalty
WECC201002228	CIP-007-1	R9	Lower/ Severe		SC	Minimal	
WECC2014013600	CIP-007-3a	R6	Lower/ Severe		SC	Minimal	
WECC2015015127	CIP-007-3a	R6	Medium/ Severe		SR	Minimal	
WECC201002213	CIP-009-1	R1	Medium/ Severe		SC	Moderate	
WECC201002214	CIP-009-1	R2	Lower/ Severe		SC	Minimal	
WECC201002215	CIP-009-1	R3	Lower/ Severe		SC	Minimal	
WECC201002216	CIP-009-1	R4	Lower/ Severe		SC	Minimal	
WECC201002217	CIP-009-1	R5	Lower/ Severe		SC	Minimal	

Common Risk Statement for all Violations

WECC determined the risk that each violation posed to the reliability of the bulk power system (BPS) as shown in the chart above. Although URE had not implemented all processes to become compliant with the requirements of the CIP Reliability Standards, WECC confirmed that URE was following government-issued guidelines that mitigated URE's risk.

Common Duration for 28 Violations

WECC determined the duration of all the violations except for WECC2014013600, WECC2015014575, and WECC2015015127 to be approximately two months to three years, from the date when each Reliability Standard became mandatory and enforceable on URE, through when URE completed each associated Mitigation Plan.

Common Certification and Verification Information for all Violations

URE certified that it had completed each Mitigation Plan, and WECC verified that URE had completed all mitigation activities

WECC201002377 CIP-003-1 R5 - OVERVIEW

WECC determined that URE failed to document and implement a program for managing access to protected Critical Cyber Asset (CCA) information, as required.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Create documentation to show the chain of authority and applicability to authorize information about and access to CCAs;
2. Identify personnel by name, title, and the information for which they are responsible for authorizing access;
3. Verify the list of personnel responsible for authorizing access to protected information at least annually;
4. Review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with URE's needs and appropriate personnel roles and responsibilities; and
5. Assess and document at least annually the processes for controlling access privileges to protected information.

WECC201002208, WECC201002209, and WECC201002210 CIP-004-1 R2, R3, and R4 - OVERVIEW

WECC determined that URE failed to: (1) establish, maintain, and document an annual training program for cyber security for personnel having authorized cyber or authorized unescorted physical access to CCAs, and review the program annually and update as necessary; (2) document a personnel risk assessment (PRA) program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access; and (3) maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Identify outstanding entity contracts that require wording modification to mandate the training of contractor and service personnel that require unescorted physical or cyber access to entity CCAs;
2. Develop contract verbiage that includes requirements for CCA training and PRA requirements;
3. Complete the training of any entity, contractor, and service personnel requiring unescorted physical or cyber access to entity CCAs; and
4. Update lists of entity, contractor, and service personnel training of personnel requiring unescorted physical or cyber access to all facilities' CCAs.

WECC2015014575 CIP-004-3 R2 - OVERVIEW

WECC determined that URE failed to maintain an annual accurate list of individuals who had cyber security training.

WECC determined the duration of the violation to be approximately 3 years and 9 months, from the date when the first instance of the missing document occurred, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Include a work order in URE's facility and equipment maintenance program to task the local reliability compliance coordinator to review the Physical Security Perimeter (PSP) access list on a monthly basis to assure that both training and background checks are current and valid. The evaluation process will highlight when an individual's training, background check, or identity verification are close to expiration to assure that the individual is either brought into compliance or removed from the access list; and
2. Perform an analysis of one facility's PSP access list to include employees, contractors, volunteers, and other entity personnel and notify the affected personnel that they require training to remain on the PSP access list.

WECC201002218 CIP-005-1 R1 - OVERVIEW

WECC determined that URE failed to ensure that every CCA resides within an Electronic Security Perimeter (ESP), and identify and document the ESPs and all access points to the perimeters.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Review each human machine interface system with the facility personnel and identify the CCAs and the ESP for each system;
2. Verify that the CCAs of each system are within an ESP;
3. Identify the access points to each ESP;
4. Update network diagrams, on separate documents, to show each system's ESP and access points;
5. Review the electronic logging narrative;
6. Review and modify the shared account review procedure;
7. Review and modify the shared account logging procedure;
8. Review and modify the electronic access procedure;
9. Review and modify the existing password narrative; and
10. Update all documents associated.

WECC201002219 and WECC201002221 CIP-005-1 R2 and R4 - OVERVIEW

WECC determined that URE failed to: (1) implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all access points to the ESP; and (2) perform a Cyber Vulnerability Assessment (CVA) of the electronic access points to the ESPs at least annually.

URE submitted its Mitigation Plans to address the referenced violations, which required URE to:

1. Specify and place purchase order for hardware and software to implement firewalls for multiplexer, digital exciter, and station service human machine interface systems;
2. Specify and place purchase order for hardware and software to replace certain hardware software at facilities;
3. Install, configure, and commission firewall hardware and software for two facilities;
4. Upgrade and incorporate hardware and software into the supervisory control and data acquisition system for two facilities;
5. Install, configure, and commission firewall hardware and software for facilities' multiplexers, digital exciters, and human machine interface systems;

6. Complete electronic access documentation, including electronic access control, of multiplexers, digital exciters, and human machine interface systems; and
7. Modify the generic data acquisition and control system (GDACS) electronic access documentation package, including electronic access control.

WECC201002220 CIP-005-1 R3 - OVERVIEW

WECC determined that URE failed to implement and document an electronic or manual process for monitoring and logging access at access points to ESPs 24 hours a day, seven days a week.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Implement and document an electronic or manual process for monitoring and logging access at access points to the ESPs 24 hours a day, seven days a week; and
2. Implement a process, where technically feasible, in which the security monitoring process detects and alerts attempts at, or actual, unauthorized accesses. These alerts will provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, review or otherwise assess access logs for attempts at, or actual, unauthorized accesses at least every 90 days.

WECC201002222 CIP-005-1 R5 - OVERVIEW

WECC determined that URE failed to review, update, and maintain all documentation to support compliance with the requirements of the Reliability Standard.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to verify that there is sufficient verbiage for the direction and review of documentation related to the Reliability Standard at least annually. If changes are necessary, URE's Mitigation Plan required URE to make relevant changes and submit the revised document for approval and signature.

WECC201002167, WECC201002205, WECC201002206, WECC201002207, and WECC201002211 CIP-006-1 R2, R3, R4, R5, and R6 - OVERVIEW

WECC determined that URE failed to: (1) document and implement the operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week; (2) document and implement the technical and procedural controls for monitoring physical access at all access points to the PSPs 24 hours a day, seven days a week; (3) record sufficient information to identify uniquely individuals and the time of access 24 hours a day, seven days a week, and failed to implement and document the technical and procedural mechanisms for logging physical entry at all

access points to the PSP; (4) retain physical access logs for at least 90 calendar days; and (5) implement a maintenance and testing program to ensure that all physical security systems under the Reliability Standard function properly.

URE submitted its Mitigation Plans to address the referenced violations, which required URE to:

1. Verify that all CCAs are contained in a PSP;
2. Verify that all access points to the PSP are identified;
3. Install additional proximity devices and associated doorway modifications;
4. Follow up on construction to mediate outstanding physical access issues;
5. Update security system test and maintenance documentation, including ports and services minimization, recovery plan, electronic access controls and monitoring, and incident response and recovery plan;
6. Complete PRA for all individuals granted cyber or unescorted physical access to physical security systems equipment;
7. Document the appropriate use of physical access controls;
8. Implement and document methods and procedures to identify and log individual's time of access to the PSP;
9. Implement and document technical and physical controls for monitoring physical access to the PSP at all access points on a 24 hours a day, seven days a week basis;
10. Document process tools and procedures to monitor physical access to the PSP;
11. Procure and develop a Physical Access Control System;
12. Request Technical Feasibility Exceptions (TFEs) for the method of controlling access to the roof at one location; and
13. Update URE's policy documents for cyber security.

WECC201002168 CIP-007-1 R1 - OVERVIEW

WECC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to test the following: GDACS master station; GDACS database server; GDACS Inter-control Center Communications Protocol (ICCP) server; GDACS domain controller; GDACS engineering station; GDACS operator view

station; GDACS engineering station; GDACS maintenance laptop; GDACS manager; event logger; and human machine interface systems.

WECC201002204 CIP-007-1 R2 - OVERVIEW

WECC determined that URE failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled;
2. Enable only those ports and services required for normal and emergency operations;
3. Disable other ports and services; and
4. File TFEs for appropriate devices.

WECC201002212 CIP-007-1 R3 - OVERVIEW

WECC determined that URE failed to establish and document a program for security patch management for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Document and implement a program for security patch management;
2. Assess security patches for applicability within 30 days of being made available;
3. Test and implement the security patches; and
4. Document compensating measures if URE does not install applicable patches.

WECC201002223 CIP-007-1 R4 - OVERVIEW

WECC determined that URE failed to use anti-virus software and other malicious software or malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to document the process for implementing anti-virus and anti-malware tools and signatures.

WECC201002224 CIP-007-1 R5 - OVERVIEW

WECC determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Review and modify existing narrative in URE's cyber security policy document and/or the document for compliance with the Reliability Standard to more clearly describe electronic logging, include the process for shared accounts, describe the process for logging the use of shared accounts, and describe the process for documenting password changing for audit purposes;
2. Ensure that each plant has an updated list documenting all levels of electronic access, including shared accounts; and
3. Update and finalize URE's policy document for cyber security and/or the document for compliance with the Reliability Standard.

WECC201002225 CIP-007-1 R6 - OVERVIEW

WECC determined that URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events related to cyber security.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Procure additional software licenses for the Cyber Assets capable of producing cyber security logs; and
2. Install the licenses at its facility and configure the agents for monitoring.

WECC201002226 CIP-007-1 R7 - OVERVIEW

WECC determined that URE failed to establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESPs as identified and documented in the Reliability Standard.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to document and implement the process for disposing or redeploying Cyber Assets within the ESP, and maintain records for the same.

WECC201002227 CIP-007-1 R8 - OVERVIEW

WECC determined that URE failed to perform a CVA of all Cyber Assets within the ESP at least annually as required.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Complete the firewall system at its facility;
2. Complete the cyber security documentation, including the CVA, for the human machine interface system at all facilities;
3. Evaluate, design, procure, and implement certain systems at its facilities;
4. Update the GDACS security documentation package to include certain systems at its facilities; and
5. Perform CVAs on all cyber systems.

WECC201002228 CIP-007-1 R9 - OVERVIEW

WECC determined that URE failed to review and update the documentation specified in the Reliability Standard at least annually, as required.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to review and update the documentation related to the Reliability Standard.

WECC2014013600 CIP-007-3a R6 - OVERVIEW

WECC determined that URE failed to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP.

WECC determined the duration of the violation to be approximately 1 month, from the date when the device to log events to the centralized logging servers at URE's facility failed, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Verify that logs are being retrieved from ICCP servers; and
2. Add a checklist to patch set installation instructions to verify that all devices where URE installs the patch continue to log to the centralized logging servers correctly.

WECC2015015127 CIP-007-3a R6 - OVERVIEW

WECC determined that URE failed to ensure that it monitored all Cyber Assets within the ESP for security events.

WECC determined the duration of the violation to be approximately 5 weeks, from the date when URE made upgrades at its facility without ensuring the monitoring of all Cyber Assets within the ESP for security events, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Update notification rules for certain cyber alerts and test the alerts in the GDACS test bed;
2. Provide updated centralized logging servers notification rules for the engineering station, and document the installation procedure and contact each point of contact at the facility;
3. Obtain and review the centralized logging servers' logs from its facilities to determine if certain cyber alerts would have been issued during the timeframe for which it was not working; and
4. Update the change request form so that it explicitly includes checkboxes related to the completion of all applicable Reliability Standard tests, and to modify the GDACS change request form.

WECC201002213 CIP-009-1 R1 - OVERVIEW

WECC determined that URE failed to create and annually review recovery plans for CCAs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to create recovery plans for CCAs that include roles and responsibilities of responders based on events of varying duration and severity.

WECC201002214 CIP-009-1 R2 - OVERVIEW

WECC determined that URE failed to exercise the recovery plans at least annually.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to exercise its recovery plan.

WECC201002215 CIP-009-1 R3 - OVERVIEW

WECC determined that URE failed to: (1) update the recovery plans to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident; and (2) communicate

updates to personnel responsible for the activation and implementation of the recovery plans within 90 calendar days of the change.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Verify that sufficient directions exist to ensure that the intended change control process is present at its facility; and
2. Make changes as necessary and submit the revised document for approval and signature.

WECC201002216 CIP-009-1 R4 - OVERVIEW

WECC determined that URE failed to include in the recovery plans processes and procedures for the backup and storage of information required to successfully restore CCAs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to implement procedures for the backup and storage of information required to restore CCAs.

WECC201002217 CIP-009-1 R5 - OVERVIEW

WECC determined that URE failed to test at least annually information essential to recovery that is stored on backup media to ensure that the information is available.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to create a process for information essential to recovery that is stored on backup media to be tested at least annually to ensure that the information is available.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed no penalty for the referenced violations. WECC considered the following factors:

1. WECC considered URE's CIP compliance history to be an aggravating factor in the disposition method for the violations described in NERC Violation IDs WECC2014013600, WECC2015014575, and WECC2015015127. WECC determined that URE's compliance history was not relevant for the violations described in NERC Violation IDs WECC201002167, WECC201002168, WECC201002204, WECC201002205, WECC201002206, WECC201002207, WECC201002208, WECC201002209, WECC201002210, WECC201002211, WECC201002212, WECC201002213, WECC201002214, WECC201002215, WECC201002216, WECC201002217, WECC201002218, WECC201002219, WECC201002220, WECC201002221, WECC201002222,

WECC201002223, WECC201002224, WECC201002225, WECC201002226, WECC201002227, WECC201002228, and WECC201002377;

2. URE voluntarily self-reported two of the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. nine violations posed a minimal, and 22 violations posed a moderate, and not a serious or substantial, risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the disposition.

After consideration of the above factors, WECC determined that, in this instance, it would issue no penalty.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[3]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[4] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that it is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[3] *See* 18 C.F.R. § 39.7(d)(4).

[4] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel, Corporate Secretary Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED

December 29, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of 28 violations[3] of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902111	CIP-002-1	R1	Medium/ Severe	GO, GOP	SR	Minimal	No Penalty
WECC200902115	CIP-002-1	R3	High/ Severe		SR	Moderate	
WECC200902116	CIP-002-1	R4	Lower/ Severe		SR	Minimal	
WECC200902133	CIP-004-1	R2	Medium/ Severe		SR	Moderate	
WECC200902130	CIP-004-1	R4	Medium/ Severe		SR	Moderate	
WECC200902120	CIP-005-1	R1	Medium/ Severe		SR	Moderate	
WECC200902121	CIP-005-1	R2	Medium/ Severe		SR	Moderate	
WECC200902124	CIP-005-1	R4	Medium/ Severe		SR	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902132	CIP-005-1	R5	Lower/ Severe	GO, GOP	SR	Minimal	No Penalty
WECC2013012269	CIP-005-3a	R3	Medium/ Severe		CA	Moderate	
WECC200902289	CIP-006-1	R1	Medium/ Severe		SR	Moderate	
WECC200902129	CIP-006-1	R2	Medium/ Severe		SR	Minimal	
WECC200902128	CIP-006-1	R3	Medium/ Severe		SR	Minimal	
WECC200902125	CIP-006-1	R4	Lower/ Severe		SR	Minimal	
WECC200902136	CIP-006-1	R6	Medium/ Severe		SR	Moderate	
WECC2013011735	CIP-006-3c	R2	Medium/ Severe		SR	Minimal	
WECC2013011732	CIP-006-3c	R4	Medium/ Severe		SR	Minimal	
WECC2013011733	CIP-006-3c	R5	Medium/ Severe		SR	Minimal	
WECC2013011734	CIP-006-3c	R6	Lower/ Severe		SR	Minimal	
WECC200902137	CIP-007-1	R1	Medium/ Severe		SR	Minimal	
WECC200902127	CIP-007-1	R2	Medium/ Severe		SR	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902126	CIP-007-1	R3	Lower/ Severe	GO, GOP	SR	Moderate	No Penalty
WECC200902140	CIP-007-1	R4	Medium/ Severe		SR	Moderate	
WECC200902141	CIP-007-1	R5	Medium/ Severe		SR	Moderate	
WECC200902146	CIP-007-1	R6	Medium/ Severe		SR	Minimal	
WECC200902148	CIP-007-1	R8	Medium/ Severe		SR	Moderate	
WECC200902149	CIP-007-1	R9	Lower/ Severe		SR	Minimal	
WECC2015015259	CIP-007-3a	R6	Medium/ Severe		SR	Minimal	

Common Risk Statement for all Violations

WECC determined the risk that each violation posed to the reliability of the bulk power system (BPS) as shown in the chart above. Although URE had not implemented all processes to become compliant with the requirements of the CIP Reliability Standards, WECC confirmed that URE was following government-issued guidelines that mitigated URE's risk.

Common Duration for 22 Violations

WECC determined the duration of 22 of the violations to be from the date when each Reliability Standard became mandatory and enforceable on URE, through when URE completed its associated Mitigation Plan.[4] The approximate durations of the violations was between two and five years.

[4] WECC200902111, WECC200902115, WECC200902116, WECC200902120, WECC200902121, WECC200902124, WECC200902125, WECC200902126, WECC200902127, WECC200902128, WECC200902129, WECC200902130, WECC200902132, WECC200902133, WECC200902136, WECC200902137, WECC200902140, WECC200902141, WECC200902146, WECC200902148, WECC200902149, and WECC20090228.

Common Certification and Verification Information for all Violations

URE certified that it had completed each Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC200902111, WECC200902115, WECC200902116 CIP-002-1 R1, R3, and R4 - OVERVIEW

WECC determined that URE failed to: (1) identify and document a risk-based assessment methodology (RBAM) to identify its Critical Assets; (2) develop a list of associated Critical Cyber Assets (CCAs) essential to the operation of the Critical Asset; and (3) approve annually the list of Critical Assets and the list of CCAs.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Conduct an engineering assessment to determine whether it possesses Cyber Assets essential to the operation of its Critical Assets;

2. Revise its RBAM and its CCA identification methodology to reflect the results of the engineering assessment; and

3. Revise and submit a list of CCAs to reflect the revised RBAM.

WECC200902133 and WECC200902130 CIP-004-1 R2 and R4 - OVERVIEW

WECC determined that URE failed to: (1) establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCAs, and review the program annually and update as necessary; and (2) maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to develop procedures establishing a training program for personnel with access to CCAs.

WECC200902120, WECC200902121, WECC200902124, and WECC200902132 CIP-005-1 R1, R2, R4, and R5 - OVERVIEW

WECC determined that URE failed to: (1) ensure that every CCA resided within an Electronic Security Perimeter (ESP), and identify and document the ESP and all access points to the perimeters; (2) implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all Electronic Access Points to the ESP; (3) perform a Cyber Vulnerability

Assessment (CVA) of the Electronic Access Points to the ESP at least annually; and (4) review, update, and maintain all documentation to support compliance with the requirements of the Reliability Standard.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Ensure that every CCA resides within an ESP and document it on drawings;

2. Implement and document the organizational processes and procedural mechanisms for control of electronic access at all points of the ESP;

3. Perform and document a CVA of the electronic access points to the ESP annually; and

4. Review, update, and maintain all documentation to support compliance with the requirements of the Reliability Standard.

WECC2013012269 CIP-005-3a R3 - OVERVIEW

WECC determined that URE failed to implement and document electronic or manual processes for monitoring and logging access at ESP access points.

WECC determined the duration of the violation to be approximately 10 months, from the date when URE failed to implement and document electronic or manual processes for monitoring and logging access at all ESP access points, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to develop, test, send, and install new software configurations at both of the facilities within scope.

WECC200902289, WECC200902129, WECC200902128, WECC200902125, and WECC200902136 CIP-006-1 R1, R2, R3, R4, and R6 - OVERVIEW

WECC determined that URE failed to: (1) document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter (PSP) 24 hours a day, seven days a week; (2) document and implement operational and procedural controls to manage physical access at all access points to the PSP 24 hours a day, seven days a week; (3) document and implement the technical and procedural controls for monitoring physical access at all access points to the PSP 24 hours a day, seven days a week; (4) log with sufficient information to identify individuals uniquely and the time of access 24 hours a day, seven days a week, and implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSP using

computer logging, video recording, or manual logging; and (5) implement a maintenance and testing program to ensure that all required physical security systems function properly.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Develop supporting documentation;
2. Accomplish adequate reviews;
3. Purchase and install communications and security hardware;
4. Install alarms at PSP access points; and
5. Configure security software.

WECC2013011735 CIP-006-3c R2 - OVERVIEW

WECC determined that URE failed to provide three of the protections required by the Reliability Standard to seven Physical Access Control System (PACS) devices. Specifically, WECC determined that URE did not have an auditable trail of use of all shared accounts for the seven PACS devices and also failed to change the password on one shared account after personnel changes. WECC also determined that URE failed to have a password of sufficient complexity for the system administration shared account. Finally, WECC determined URE's CVA for the seven PACS devices did not include a review of ports and services, a review of default accounts, or an action plan to remediate or mitigate vulnerabilities identified in the assessment as required.

WECC determined the duration of the violation to be 3 years and 7 months, from the date when URE failed to provide all required protections to seven PACS devices, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Complete ports and service analysis on the test platform;
2. Investigate ports and services on PACS system;
3. Update and complete CVA on PACS system;
4. Disable unnecessary services on PACS system;

5. Identify all shared accounts and issue individual user accounts to personnel who do not need to use shared accounts to ensure continuity of operations;

6. Study the feasibility of having its security contractor use individual user accounts rather than shared user accounts;

7. Remove shared administrator accounts, except where it is not technically feasible to use individual administrator accounts;

8. Implement a policy or procedure to ensure that shared account passwords are changed any time a shared account user leaves the organization;

9. Implement regularly scheduled password changes;

10. Provide additional training on the requirements of CIP Reliability Standards to the employees responsible for the system administration of PACS, along with their first- and second-line supervisors. Further, provide training on the importance of the CVA to cyber security and the necessity of effective and accurate communication to URE's culture of compliance; and

11. Change the PACS password to ensure that it meets the minimum complexity requirements.

WECC2013011732 CIP-006-3c R4 - OVERVIEW

WECC determined that URE failed to implement the operational and procedural controls to manage physical access to two PSPs 24 hours a day, seven days a week.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the operational and procedural controls, through when URE implemented the proper methods to control physical access to the two PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Immediately secure the control room and cable spreading room doors;

2. Install restricted key lock cores on the control room and cable spreading room doors; and

3. Restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

WECC2013011733 CIP-006-3c R5 - OVERVIEW

WECC determined that URE failed to implement the technical and procedural controls for monitoring physical access at three access points as required.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the technical and procedural controls for monitoring physical access to three access points to the PSPs, through when URE implemented the proper methods to monitor physical access to the PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Immediately secure the control room and cable spreading room doors;

2. Install restricted key lock cores on the control room and cable spreading room doors; and

3. Restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

WECC2013011734 CIP-006-3c R6 - OVERVIEW

WECC determined that URE failed to implement the technical and procedural controls for logging physical access at three access points as required.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the technical and procedural controls for monitoring physical access to three access points to the PSPs, through when URE implemented the proper methods to control physical access to the PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

WECC200902137, WECC200902127, and WECC200902126, CIP-007-1 R1, R2, and R3 - OVERVIEW

WECC determined that URE failed to: (1) ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls; (2) establish, document, and implement a process to ensure that it only enabled those ports and services required for normal and emergency operations; and (3) establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Perform a CVA on the supervisory control and data acquisition (SCADA) system;

2. Complete investigation of ports and services on the generic data acquisition and control system (GDACS) system;

3. Disable unnecessary ports and services on the SCADA system, where possible, and update the system baseline to include all ports and services;

4. Complete full port scans;

5. Ensure that, for GDACS Cyber Assets within an ESP, it enabled only ports and services required for normal and emergency operations, and disabled all other ports and services; and

6. Assess security patches.

WECC200902140, WECC200902141, WECC200902146, WECC200902148, and WECC200902149 CIP-007-1 R4, R5, R6, R8, and R9 - OVERVIEW

WECC determined that URE failed to: (1) use anti-virus software and other malicious software or malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP; (2) establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access; (3) ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor cyber security system events; (4) perform a CVA of all Cyber Assets within the ESP at least annually as required; and (5) review and update the documentation specified in the Reliability Standard at least annually.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Perform a new CVA with an updated execution status;

2. Complete investigation of ports and services on the GDACS system;

3. Disable unnecessary ports and services on the SCADA system, where possible, and update the system baseline to include all ports and services;

4. File Technical Feasibility Exceptions for all remaining GDACS devices that are not capable of enforcing strong passwords;

5. Adopt a standard form for tracking shared account use;

6. Complete disabling unused ports and services identified;

7. Complete disabling all default accounts identified;

8. Complete CVA for all GDACS Cyber Assets within an ESP; and

9. Formally document default account review for all GDACS Cyber Assets within an ESP.

WECC2015015259 CIP-007-3a R6 - OVERVIEW

WECC determined that URE failed to ensure all Cyber Assets within the ESP had automated tools or organizational process controls to monitor system events related to cyber security.

WECC determined the duration of the violation to be ten months, from the date when URE upgraded its SCADA computers' operating systems without enabling all required alert alarms, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to correct the alarming problem, test it on an off-line test platform, and install the correct configuration.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed no penalty for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's CIP compliance history to be an aggravating factor in the disposition method for the violations described in NERC Violation IDs WECC2013011732, WECC2013011733, WECC2013011734, WECC2013011735, and WECC2015015259. WECC determined that URE's compliance history was not relevant for the violations described in NERC Violation IDs WECC200902111, WECC200902115, WECC200902116, WECC200902120, WECC200902121, WECC200902124, WECC200902125, WECC200902126, WECC200902127, WECC200902128, WECC200902129, WECC200902130, WECC200902132, WECC200902133, WECC200902136, WECC200902137, WECC200902140, WECC200902141, WECC200902146, WECC200902148, WECC200902149, WECC200902289, and WECC2013012269;

2. URE voluntarily self-reported 27 of the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. fourteen violations posed a minimal, and 14 violations posed a moderate, and not a serious or substantial, risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the disposition.

After consideration of the above factors, WECC determined that, in this instance, it would issue no penalty.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the disposition is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

---

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel, Corporate Secretary Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

December 29, 2016

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP17-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

NERC respectfully requests that the Commission accept this Spreadsheet NOP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Associate Director,
Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
2	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2015015210	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
2	SERC_URE1 submitted a Self-Report stating that it was in violation of CIP-005-3a R1.5. SERC_URE1 failed to afford the electronic access control and monitoring (EACM) Cyber Assets the protective measures specified in CIP-007-3a R8, by failing to conduct a cyber vulnerability assessment (CVA) on the EACM Cyber Assets for one year. As part of mitigation for a prior violation, SERC_URE1 conducted a CVA. However, the CVA that SERC_URE1 conducted was limited to the ESP access points, Critical Cyber Assets (CCAs), and non-critical Cyber Assets within the ESP. As a result, SERC_URE1 failed to conduct a CVA on the EACM devices that year. In total, SERC_URE1 failed to perform CVAs for all of its EACM devices. Prior to this issue, SERC_URE1 last conducted a CVA that included the EACM devices the year before. SERC_URE1 discovered this issue while preparing for the next year's CVA. In all prior years, SERC_URE1 performed the CVA for all Cyber Assets in scope at the same time. During the year at issue, SERC_URE1 assumed that the CVA addressed all Cyber Assets requiring a CVA (as it had done in all previous years) and failed to make the distinction that not all involved Cyber Assets in scope of the CVA were included. Due to this mistake, SERC_URE1 did not conduct the required CVA for EACM devices. The root cause of this violation was a misunderstanding of the CVA scope and the Cyber Assets that were to be included in the year's CVA effort. The duration of the violation was approximately eight months.	CIP-005-3a	R1.5	Medium	Severe

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
2	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, SERC_URE1's failure to conduct a CVA on the EACMs could have allowed security vulnerabilities to go unidentified, remaining available for exploitation for an extended period. However, SERC_URE1 annually reviewed and changed the passwords for all EACM devices and accounts in service that are part of this instant issue. SERC_URE1 reviewed the existing ports and services several times the year of the violation. Modifying the EACM network switch ports and services requires a serial connection, meaning that a person must be physically located at the Cyber Asset to make modifications. SERC_URE1's logs show that its EACM network switches were accessed only three times, all by personnel who were authorized for such access. SERC_URE1 also secures all the affected EACM Cyber Assets within a firewall secured subnet with no remote access permitted, restricting potential attack vectors. If an unauthorized individual gained physical access to the EACM devices, the individual would still need a password to access the servers, workstations, and the application software. SERC_URE1 completely isolates the EACM subnet from the network containing CCAs, limiting any potential crossover impacts that could affect or degrade the energy management system.	One day after SERC_URE1 failed to conduct a CVA covering EACM devices for the year at issue.	When SERC_URE1 conducted the next year's CVA, which included the EACM devices.

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
2	$50,000 (for SERC2015015209, SERC2015015210, SERC2016015560, and SERC2016015561)	Self-Report	To mitigate this violation, SERC_URE1: 1) completed the required CVA on the EACM Cyber Assets; and 2) established an internal control to monitor the completion of the annual CVA.	8/31/2015	11/18/2016

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's compliance history to be an aggravating factor in the penalty determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
3	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2015015209	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	SERC_URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R2.2. SERC_URE1 failed to afford the physical access control system (PACS) Cyber Assets the protective measures specified in CIP-007-3a R8, by failing to conduct a cyber vulnerability assessment (CVA) on the PACS Cyber Assets for one year. As part of mitigation for a prior violation, SERC_URE1 conducted a CVA. However, the CVA that SERC_URE1 conducted was limited to the ESP access points, Critical Cyber Assets (CCAs), and non-critical Cyber Assets within the ESP. As a result, SERC_URE1 failed to conduct a CVA on the PACS devices for the year at issue. In total, SERC_URE1 failed to perform CVAs for all of its PACS devices. Prior to this violation, SERC_URE1 last conducted a CVA that included the PACS devices the year before. SERC_URE1 discovered this violation while preparing for the next year's CVA. In all prior years, SERC_URE1 performed the CVA for all Cyber Assets in scope at the same time. During the year at issue, SERC_URE1 assumed that the CVA addressed all Cyber Assets requiring a CVA to be conducted (as it had done in all previous years) and failed to make the distinction that not all involved Cyber Assets in scope of the CVA were included. Due to this, SERC_URE1 did not conduct the required CVA for PACS devices. The root cause of this violation was a misunderstanding of the CVA scope and the Cyber Assets that were to be included in the year's CVA effort. The duration of the violation was approximately eight months.	CIP-006-3c	R2.2	Medium	Severe
3					

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
3	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, SERC_URE1's failure to conduct a CVA on the PACS devices could have allowed security vulnerabilities to go unidentified, remaining available for exploitation for an extended period. However, SERC_URE1 annually reviewed and changed the passwords for all PACS devices and accounts that were part of this violation. Additionally, SERC_URE1 reviewed the existing ports and services several times that year. The PACS door controllers are firmware-based appliances and, as such, require firmware changes to update any ports and services in use and on the baseline. No firmware updates were made for the door controllers during the violation. SERC_URE1 also secures all the affected PACS Cyber Assets within a firewall secured subnet with no remote access permitted, restricting potential attack vectors. SERC_URE1 completely isolates the PACS subnet from the network containing CCAs, thereby limiting any potential crossover impacts that could affect or degrade the energy management system.	One day after SERC_URE1 failed to conduct a CVA covering PACS devices for the year at issue.	When SERC_URE1 conducted the next year's -CVA, which included the PACS devices.

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
3	$50,000 (for SERC2015015209, SERC2015015210, SERC2016015560, and SERC2016015561)	Self-Report	To mitigate this violation, SERC_URE1: 1) completed the required CVA on the PACS Cyber Assets; and 2) established and calendared an internal control task to monitor future completion of CVAs for the Cyber Assets at issue in this violation.	8/31/2015	11/18/2016

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
3	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's compliance history to be an aggravating factor in the penalty determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
4	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2016015560	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	During a Compliance Audit, SERC determined that SERC_URE1 was in violation of CIP-005-3a R1.5. SERC_URE1 failed to properly identify several servers as Electronic Access Control and Monitoring Systems (EACMS) and thus could not provide evidence that it afforded the servers the protective measures specified in CIP-005-3a R1.5. SERC_URE1 used servers on the corporate network to maintain logs of access to the ESP firewalls and to generate alerts and reports as part of monitoring access at ESP access points, as required by CIP-005-3a R3. SERC_URE1 interpreted the required logging function and the required monitoring function in CIP-005-3a R3 to be two separate and distinct functions, with only the latter falling under CIP-005-3a R1.5. However, in addition to using these server reports to demonstrate compliance, SERC_URE1 also manually reviewed these reports each day and issued alerts based on issues identified in that review. Since SERC_URE1 manually reviewed these reports and generated alerts based on that review, SERC_URE1 should have identified these servers as EACMS. SERC_URE1 normally used servers to perform this function, one in the primary control center and one in the back-up control center. However, during the Compliance Audit, SERC_URE1 was in the process of replacing the original servers with newer ones, and had them all in service and operational for approximately two to three months. The root cause of this violation was a misinterpretation by SERC_URE1 of the Standard and Requirement. The duration of the violation was approximately two and a half years.	CIP-005-3a	R1.5	Medium	Severe
4					

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
4	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, SERC_URE1's failure to identify and protect the EACMS servers could have led to compromised servers, the inability to generate alerts for unauthorized access to CIP assets, and the inability to detect successful unauthorized access attempts. However, SERC_URE1's firewalls performed both 'access to' and 'access through' monitoring and alerting. The firewalls operated independently from the servers so that they would have remained operational if the servers had failed.	When the audit period began.	Mitigation Plan completion.

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
4	$50,000 (for SERC2015015209, SERC2015015210, SERC2016015560, and SERC2016015561)	Compliance Audit	To mitigate this violation, SERC_URE1: 1) designated the involved servers as EACMs under Version 5 of the CIP Standards; and 2) sent an email to responsible staff to make them aware that the servers are properly considered EACMs.	7/1/2016	11/18/2016

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
4	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC determined SERC_URE1's compliance history should not serve as a basis for aggravating the penalty.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
5	SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2016015561	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
5	During a Compliance Audit, SERC determined that SERC_URE1 was in violation of CIP-006-3c R1.6.1. SERC_URE1 failed to maintain visitor logs that documented the date and time of visitors' entry and exit, including the date and time, to and from two Physical Security Perimeters (PSPs). The SERC audit team reviewed visitor access logs for the SERC_URE1 control center PSPs and found multiple logging issues with the manual log-books, including incomplete lines within the logs and missing sign-in times or sign-out times dating back approximately one year. Specifically, SERC_URE1 failed to log entry and exit times on multiple occasions, including for large groups of student visitors on tours, for which SERC_URE1 only documented the entry and exit dates. The root cause of this violation was multiple human performance failures, in which SERC_URE1 employees failed to follow documented procedures for appropriate logging visitors to the PSP. The duration of the violation was approximately a year and a half.	CIP-006-3c	R1.6.1	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
5	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Specifically, if a problem or issue arose, SERC_URE1's failure to maintain complete visitor logs would make any forensic review difficult, because there would be an incomplete log of who was within the secured area at the time. However, SERC_URE1 had several security measures in place to protect the PSP. For example, SERC_URE1 had live video surveillance cameras covering some areas of the PSPs and could view this footage in real time. Further, SERC_URE1 staffed its control centers twenty-four hours a day, seven days a week. To gain access to the PSP in question, an individual would first have to pass through a carded gate arm.	The first documented log in which SERC_URE1 failed to properly log visitors to the PSP.	When SERC_URE1 revised its logging form and provided training on visitor logging to employees.

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
5	$50,000 (for SERC2015015209, SERC2015015210, SERC2016015560, and SERC2016015561)	Compliance Audit	To mitigate this violation, SERC_URE1: 1) modified the form used to log visitor access to provide separate columns for the date and time of ingress and egress for visitors; 2) placed an increased emphasis on visitor logging in the annual cyber training that is required of all employees with access to PSPs; 3) provided additional awareness of logging requirements, through periodic reminders on SERC_URE1 digital signage; and 4) constructed a new facility that houses the primary energy control center and support staff. The new facility significantly reduced the number of PSP doorways.	9/8/2016	11/18/2016

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
5	Neither Admits nor Denies	SERC reviewed SERC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. SERC considered SERC_URE1's compliance history and determined that there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
6	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2015015024	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
6	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R1. Specifically, for the first instance; WECC_URE1 reported that, two third-party vendor Security Officers (Officer A and Officer B) with authorized NERC unescorted physical access rights, assumed the responsibility as "escorts" for visiting contract personnel to the control center. Officer A escorted four contractors through the Physical Security Perimeter (PSP) via a card reader (CR) into an enclosed hatch room located behind the control room. Six minutes after Officer A escorted four contractors, Officer B escorted three different contractors into the control center PSP via a CR. Once all three contractors were in the PSP, Officer B exited the PSP via a CR, leaving the three contractors inside the PSP without an escort. The three contractors remained in camera view until Officer A appeared on-screen approximately four minutes later to continue his escorting duties. Officer A appeared on-screen without his original four assigned visitors that he had previously escorted into the hatch room. This same type of activity occurred multiple times throughout the day during an approximately three hour period. WECC determined that per CIP-006-3a R1.6, WECC_URE1 failed to continuously escort the visitors, as required by WECC_URE1's visitor control program, for approximately three hours. For the second instance, WECC_URE1 reported that, a third-party vendor Security Officer (Officer X) arrived at the control center to perform NERC monitoring duties. Officer X arrived without his company-issued ID Badge. Officer X had completed his required NERC CIP training, but his access order to provision authorized unescorted physical access to PSPs was not yet approved. Therefore, Officer X was considered a visitor and was to be continuously escorted by personnel with authorized unescorted physical access to PSPs. Two other Security Officers (Officer Y and Officer Z) assumed escorting responsibilities over Officer X. Approximately three minutes after Officer X arrived, Officer Y and Officer Z escorted Officer X, along with two contractors into the control center PSP via a CR. Approximately six minutes later, Officer Y exited the PSP alone. Officer Z and Officer X were in the PSP together with the contractors, and Officer Z assumed sole escorting responsibility over Officer X and the contractors. Approximately six minutes later, Officer Z escorted the two contractors out of the PSP, leaving Officer X without an escort while in the PSP for approximately two more hours. WECC determined that per CIP-006-3a R1.6, WECC_URE1 failed to continuously escort the visitor, as required by WECC_URE1's visitor control program, for approximately two and a half hours. The root cause of both issues was failure of WECC_URE1's third-party vendor to adhere to their contractual agreement.	CIP-006-3c	R1; R1.6	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
6	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE1 failed to ensure continuous escorting of unauthorized visitors within a PSP, which could allow said access to go unnoticed and unchecked. Such access may then be used to cause harm to Critical Cyber Assets (CCAs) essential to the operation of the BPS, thereby potentially negatively affecting the BPS. In both instances, WECC_URE1 had video monitoring of the visitors in scope and verified no malicious activity occurred. In the second instance, the security officer's authorized access was pending approval, he had an approved personnel risk assessment (PRA), and he had the required NERC CIP training. Additionally, related to the first instance, WECC_URE1's control center is continuously manned and the CCAs were continuously monitored, thereby reducing the risk of actions that could negatively affect the BPS.	The first instance began when the contractors were left inside the PSP unescorted The second instance began when the Security Officer was left inside a PSP unescorted	The first instance ended approximately three hours later when WECC_URE1 resumed escorting of the contractors within the PSP The second instance ended approximately two and a half hours later when WECC_URE1 resumed escorting of the security officer within the PSP

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
6	$60,000 (for WECC2015015024 and WECC2016015456)	Self-Report	To mitigate this violation, WECC_URE1: 1) resumed the escorting of the contractors within the PSP; 2) resumed the escorting of the security officer within the PSP; and 3) held meetings with its contract service provider's leadership team reminding them of their contractual obligations as outlined in WECC_URE1's Master Service Agreement to abide by NERC CIP Standards and WECC_URE1's visitor control program, which includes specific guidelines for accessing NERC-Restricted areas.	8/21/2015	7/1/2016

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
6	Agrees/Stipulates	Credit was not given for WECC_URE1's internal compliance program (ICP). Although WECC_URE1 has a documented ICP that has been provided to WECC, it is Enforcement's belief that had the ICP been implemented properly, WECC_URE1 would have been able to identify, assess, and correct this violation in a timely manner. WECC_URE1 discovered the first instance of this violation and self-reported 161 days after discovery. Therefore, Enforcement did not apply self-reporting credit to the penalty amount for this issue. WECC considered WECC_URE1's compliance history in determining the penalty. WECC considered WECC_URE1's compliance history to be an aggravating factor in the penalty determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
7	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2016015456	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
7	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-006-3c R1. Specifically, for the first instance, WECC_URE1 reported that an employee (Employee A) with authorized unescorted physical access rights to a PSP, assumed the responsibility of an escort for an Information Technology (IT) employee (Employee B) that did not have unescorted physical access rights to the PSP. Employee A escorted Employee B into the PSP and signed him into the NERC CIP Visitor Log. Employee B was inside the PSP to replace Employee A's computer and copy files from the old to the new computer. Employee A left Employee B in his office, unescorted, ~~from~~ for approximately fifteen minutes and a second time for approximately thirty minutes. It was not until Employee A escorted Employee B out of the PSP that Employee A realized the oversight and immediately contacted the NERC CIP Compliance team to report the incident. WECC determined that per CIP-006-3a R1.6, WECC_URE1 failed to continuously escort Employee B, as required by WECC_URE1's visitor control program, for approximately 45 minutes. For the second instance, WECC_URE1 reported that, a third-party vendor Security Officer (Officer A) with authorized unescorted physical access rights to a PSP assumed the responsibility of an escort for another third-party vendor Security Officer (Officer B), who did not have unescorted physical access rights to the PSP. Officer B was supposed to be stationed at the exterior of the PSP cage to perform manual monitoring for a planned outage to the badge system. Officer A incorrectly stationed Officer B, inside the PSP cage. Approximately five minutes later, the operations center received a call from a power system operator to report that Officer B had been left unescorted inside the PSP cage. The operations center operator immediately contacted the PSP Security and requested they escort Officer B out of the PSP cage, which was completed at approximately ten minutes. Due to the NERC in-person training completed by the power system operator, he quickly recognized the unescorted Security Officer's presence in the PSP was a problem and reported the situation to the operations center. WECC determined that per CIP-006-3a R1.6, WECC_URE1 failed to continuously escort Officer B, as required by WECC_URE1's visitor control program, for approximately 20 minutes. The root cause of the first issue was a lapse in judgement by one employee for not remembering proper escorting procedures previously trained on as part of the mitigation for WECC2015015024. The root cause of the second issue was lack of a third-party vendor adhering to the contractual agreement.	CIP-006-3c	R1; R1.6	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
7	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE1 failed to ensure continuous escorting of unauthorized visitors within a PSP which could allow said access to go unnoticed and unchecked. Such access could be used to cause harm to CCAs essential to the operation of the BPS, thereby negatively affecting the BPS. In both instances, the unescorted employee and the Security Officer did not have electronic access to Critical Cyber Assets (CCAs). Additionally, the unescorted employee and the Security Officer were not left entirely alone in the PSP, as it was occupied by other employees who were authorized to be there.	The first instance began when an employee was left unescorted within a PSP The second instance began when a Security Officer was left inside a PSP unescorted	The first instance ended on approximately 45 minutes later when WECC_URE1 resumed escorting of the employee within the PSP The second instance ended when approximately 15 minutes later WECC_URE1 removed the Security Officer from the PSP

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
7	$60,000 (for WECC2015015024 and WECC2016015456)	Self-Report	To mitigate this violation, WECC_URE1: 1) resumed the escorting of the employee within the PSP; 2) had the individual involved in the first incident recall and re-review the visitor escort pamphlet, thus retraining themselves on the proper visitor escort protocol for a NERC CIP PSP; 3) completed the “PSP footprint reduction” project, which reduced the number of people whose regular work location was within a PSP; 4) removed the Security Officer from the PSP; 5) held meetings with its contract service provider's leadership team reminding them of their contractual obligations as outlined in WECC_URE1's Master Service Agreement to abide by NERC CIP Standards and WECC_URE1's visitor control program, which includes specific guidelines for accessing NERC-Restricted areas; and 6) worked with its security vendor to implement an internal control of a recording on its toll-free start-of-shift telephone line. The recording states that officers assigned to provide physical security during a scheduled outage of the badge system are never permitted to enter a PSP, unless they are currently cleared by WECC_URE1 and possess their NERC ID badge, or they are escorted continuously by an individual who is authorized with unescorted physical access to the PSP.	12/22/2015	10/13/2016

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
7	Agrees/Stipulates	Credit was not given for WECC_URE1's internal compliance program (ICP). Although WECC_URE1 has a documented ICP that has been provided to WECC, it is Enforcement's belief that had the ICP been implemented properly, WECC_URE1 would have been able to identify, assess, and correct this violation in a timely manner. WECC considered WECC_URE1's compliance history in determining the penalty. WECC considered WECC_URE1's compliance history to be an aggravating factor in the penalty determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
8	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC200901795	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
8	During a Spot Check, WECC determined that WECC_URE2 was in violation of CIP-004-1 R4. WECC determined that WECC_URE2 failed to maintain lists of personnel containing specific electronic access rights to Critical Cyber Assets (CCAs). WECC reviewed the WECC_URE2 documentation for evidence of compliance with the Standard and determined there was insufficient documentation of cyber access rights. Specifically, the documentation described only general access rights to systems within the Electronic Security Perimeter (ESP) and did not include the specific electronic access rights to CCAs as required by the Standard. Furthermore, WECC_URE2 produced two documents listing system users; however, the lists failed to identify the specific systems for which these individuals had access. A subsequent data request for more detailed documentation of specific electronic access rights failed to demonstrate compliance with the Standard. WECC also reviewed documentation demonstrating quarterly reviews of personnel with access to CCAs. WECC reviewed WECC_URE2's perimeter access review documents for each quarter during a period of a year. WECC found that the document did not provide details on all personnel that were included in the previous and following quarterly reviews. Specifically, personnel were missing from the quarterly review. WECC_URE2 produced no additional evidence to demonstrate a change in personnel access rights between the quarters. While reviewing the same lists, WECC also identified one WECC_URE2 employee that had a change in physical access rights, however no documentation was provided to confirm an update to the access lists was made within seven days of the change in access rights. WECC issued a data request to WECC_URE2 to determine if the lists had been updated within seven days as required by the Standard. Based on the response provided by WECC_URE2, WECC determined that its lists had not been updated within seven days of the change in access rights. Based on documentation, interviews and observation, WECC determined that WECC_URE2 had a violation of CIP-004-1 R4 because it failed to maintain lists containing detailed specific electronic access rights for personnel with authorized cyber access to CCAs. WECC also confirmed that WECC_URE2 failed to review access lists on a quarterly basis because its review did not include all individuals with physical access rights during the previous and following reviews. Additionally, WECC_URE2 failed to update access lists within 7 days of a change of access rights for one individual as required by the Standard. WECC completed a Reliability Standard Audit Worksheet (RSAW) detailing the findings and evidence reviewed	CIP-004-1	R4	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
8	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE2 failed to maintain, update, and review access lists containing specific electronic and physical access rights for all personnel with access to CCAs as required by the Standard. The error could lead to personnel without authorized access rights, achieving or retaining access privileges to CCAs. WECC_URE2 had partially mitigated the risk by implementing a new access control system during the same quarter it failed to perform the quarterly review. Furthermore, WECC_URE2's non-specific electronic access controls reduce the likelihood of non-authorized system usage.	WECC_URE2's Mitigation Plan completion date for an earlier violation of the same standard	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
8	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Spot Check	To mitigate this violation, WECC_URE2: 1) reviewed the CCA Access Control List and ensure removal of access is occurring as specified in CIP-004-1 R4; 2) performed and properly documented quarterly reviews of the CCA Access Control List; and 3) ensured specific logical access for each CCA is documented in the quarterly reviews.	3/19/2010	9/1/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
8	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE2's compliance history in determining the disposition track.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
9	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC200901796	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	During a Spot Check, WECC determined that WECC_URE2 was in violation of CIP-007-1 R1. WECC determined that WECC_URE2 failed to implement cyber security test procedures and document testing results pursuant to CIP-007-1 R1. During the CIP Spot Check, WECC reviewed documents provided by WECC_URE2 to demonstrate compliance with CIP-007-1 R1. WECC_URE2 provided over 30 documents to demonstrate compliance with this Standard, including its current change and configuration management plan used to enforce testing procedures and change management. WECC_URE2 also provided its former process documents used for this Standard during an earlier part of the compliance review period. Based on the documentation provided, WECC determined that WECC_URE2 failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) do not adversely affect existing cyber security controls. Specifically, WECC determined that WECC_URE2 failed to implement cyber security test procedures and document testing results as required by CIP-007-1 R1.1. Prior to approximately six months before the audit, WECC_URE2 did not have a procedure for testing the affect of new Cyber Assets or significant changes to existing Cyber Assets within the ESP on existing security controls. WECC based this finding on WECC_URE2's cyber security test procedures document, which did not have cyber security test procedures for significant changes to Critical Cyber Assets (CCAs) within the ESP. WECC_URE2 later introduced revised cyber security test procedures that had a procedure for testing existing security controls; however, no evidence was provided to demonstrate that this procedure was followed as documented. WECC also discovered that WECC_URE2 failed to provide documentation that its test environment reflected the production environment, as required by CIP-007-1 R1.2. Although WECC_URE2's test environment was within its ESP, it provided no base configuration documentation to establish similarities and deltas between production and test environments. Furthermore, WECC found no evidence that WECC_URE2 was documenting security control tests when significant changes were made to critical cyber assets CCAs, as required in R1.3. As a result, no documented test results were available to validate that users or system accounts retained the proper permissions after system changes were implemented.	CIP-007-1	R1	Medium	Severe
9	Based on documentation, interviews and observation, WECC determined that WECC_URE2 had a violation of CIP-007-1 R1 because WECC_URE2 failed to implement cyber security test procedures and document testing results as required by CIP-007				

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
9	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this situation, WECC_URE2 failed to have procedures to determine what affect significant changes to Cyber Assets would have on existing cyber security controls. Despite the absence of a formal process, it is noted that WECC_URE2 did check for vulnerabilities in another manner. In the event of a planned change, WECC_URE2 performed scans and completed a worksheet with change management steps. Although this process is not sufficient to demonstrate compliance, it does reduce the potential impact of changes to existing security controls.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
9	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Spot Check	To mitigate this violation, WECC_URE2: 1) examined the change control process documentation and ensured that the process for testing cyber security controls is adequate; 2) updated the base configuration documentation to establish similarities and deltas between production and test environments; 3) modified test and change control procedures to better capture evidence showing the risks and effects of the deltas between production and test environments; 4) modified documentation on how test environments are maintained and controlled; and 5) developed procedures to ensure a direct mapping between execution evidence and the cyber controls tests, which will also include the collection of cyber security test results.	3/30/2010	9/1/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
9	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
10	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102961	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
10	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-007-1 R3. During an on-site audit, WECC discussed with WECC_URE2 its Self-Report. According to WECC, WECC_URE2 stated that it failed to assess patches for 20 Critical Cyber Assets (CCAs) within 30 days of availability of the patches. Specifically, WECC_URE2 stated that it failed to assess patches for ten converters and ten routers. WECC determined that WECC_URE2 was in violation of CIP-007-1 R3 for failing to assess security patches on 20 of its CCAs within 30 days of the patches being available. The cause of the violation was that WECC_URE2's personnel responsible for assessing patches were not on the vendor mailing list for the devices in scope, so were not getting the notifications for when patches are available.	CIP-007-1	R3; R3.1	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
10	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to assess security patches may result in vulnerabilities remaining unaddressed for extended periods of time. In this case, WECC_URE2 failed to assess, within 30 days, security patches for 20 of its CCAs used for access control and monitoring of ten Electronic Security Perimeters. As a compensating measure, WECC_URE2 has strong technical and procedural controls that may limit exposure of the CCAs involved in this violation to improper or malicious use. In addition, each of the CCAs involved in the violation are located in Physical Security Perimeters, which also serves to reduce the changes that the CCAs are subject to improper or malicious use.	when the Standard became mandatory and enforceable on WECC_URE2	when WECC_URE2 performed the required security patch assessments

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
10	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Self-Report	To mitigate this violation, WECC_URE2: 1) implemented a program to check periodically for upgrades and patches; 2) completed assessment of previous releases; 3) tested and installed all applicable patches and upgrades on all affected devices; and 4) assigned the lead communications engineer and maintenance reliability compliance coordinator to check the vendor websites on a 30-day basis and upon discovery of a new patch release the patch will be assessed for applicability.	8/24/2011	5/10/2012

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
10	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC_URE2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
11	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102962	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-007-1 R5. During an on-site audit, WECC discussed with WECC_URE2's its Self-Report. According to WECC, WECC_URE2 stated that it failed to rename default accounts on two Critical Cyber Assets (CCAs) as required by CIP-007-1 R5.2.1. In this regard, WECC_URE2 did change the password of the default administration account as required by CIP-007 R5.2.1, but it did not rename the account on two CCAs. WECC_URE2 also failed to provide an audit trail of account use for its shared accounts as required by CIP-007-1 R5.2.3. Finally, WECC_URE2 failed to change passwords on 16 of its CCAs as least annually, as required by CIP-007-1 R5.3.3. According to WECC, WECC_URE2 misinterpreted the requirement to apply only to "user" and "administrative" accounts instead of all accounts including maintenance, shared, administrator, and system accounts. Passwords for user and administrative accounts were rotated but some maintenance accounts on specific machines were not rotated as per the requirement. The Supervisory Control and Data Acquisition (SCADA) manager determined that the Windows system administrator misunderstood which accounts required a modification of passwords annually and when personnel changes occurred. WECC determined that WECC_URE2 is in violation of CIP-007-1 R5.2.1 for failing to rename default accounts on two CCAs, CIP-007-1 R5.2.3 for failing failed to provide an audit trail of account use for its shared accounts, and CIP-007-1 R5.3.3 for failing to change passwords on sixteen of its CCAs at least annually. The cause was a misunderstanding of the requirement.	CIP-007-1	R5; R5.2.1; R5.2.3; R5.3.3	Medium	Severe
11					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
11	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to establish technical and procedural controls to ensure that account and user access is implemented in compliance with CIP-007-1 R5 may allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. As compensating measures, WECC_URE2 has established strong technical and procedural controls that limit the risk of exposure to the CCAs identified. The physical and logical controls for these devices are limited to its personnel that have been provisioned access via its change control and management, personnel risk assessment, and CIP training programs. WECC_URE2 has also established strong technical and procedural controls that limit the risk of exposure to the CCAs identified.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
11	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Self-Report	To mitigate this violation, WECC_URE2: 1) reviewed all system accounts and passwords to determine when the last time passwords were changed; 2) modified passwords and account names, where appropriate; 3) created a process for the SCADA manager to create a new user workbook report for quarterly account review; and 4) used a new version of the energy management system (EMS) system that does not require passwords and account name s to be embedded in the EMS code.	3/23/2012	6/28/2012

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
11	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC_URE2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
12	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102963	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-007-1 R6. During an on-site audit, WECC discussed with WECC_URE2 its Self-Report. According to WECC, WECC_URE2's process for managing cyber security events monitoring is documented. However, WECC_URE2 could not produce evidence that it monitored for security events on 21 Critical Cyber Assets (CCAs). WECC_URE2, while implementing and documenting the organizational processes and technical and procedural mechanisms for monitoring for security events, did not do so for "all" Cyber Assets within the Electronic Security Perimeter (ESP). Because WECC_URE2 could not provide evidence that it monitored for security events on the above CCAs, WECC concluded that WECC_URE2 was in violation of CIP-007-1 R6. WECC determined that WECC_URE2 was in violation of CIP-007-1 R6 because it could not provide evidence that it monitored security events on the above CCAs, as required by CIP-007-1 R6.1. The cause was that the cyber assets were configured to send logs to the incorrect IP address. Therefore, the centralized logging server was not receiving the logs. The IP was also configured with the old IP address of the syslog server due to a miscommunication between the IT and maintenance groups.	CIP-007-1	R6; R6.1	Medium	Severe
12					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
12	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Failure to implement security controls to monitor cyber security system events, may allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. In addition, such access may then be used to cause harm to CCAs essential to the operation of the Bulk Electric System, thereby potentially negatively affecting the BPS. As compensating measures, WECC_URE2 had established strong technical and procedural controls that limit the risk of exposure to the CCAs identified. The physical and logical controls for these devices are limited to its personnel that have been provisioned access via its change control and management, personnel risk assessment, and CIP training programs.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
12	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Self-Report	To mitigate this violation, WECC_URE2 went to the affected locations and made configuration changes such that all devices listed in the Self-Report were logging to the security event server.	10/3/2011	5/10/2012

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
12	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC_URE2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
13	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2013012054	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
13	WECC_URE2 submitted a Self-Certification stating that it was in violation of CIP-006-1 R1. Specifically, WECC_URE2 reported that it failed to identify 15 devices as Critical Assets used in the access control and monitoring of its Physical Security Perimeters (PSPs). WECC_URE2 reported that because the devices were not properly identified as Physical Access Control and Monitoring (PACM) devices, the devices did not receive the protections required by CIP-006-1 R1, specifically R1.8. A WECC Subject Matter Expert (SME) reviewed WECC_URE2's Self-Certification. As part of the review, the SME requested additional information from WECC_URE2 concerning the violation. Based on a review of all information received, the SME determined that WECC_URE2 was in violation of CIP-006-1 R1, specifically R1.8. The SME determined that WECC_URE2 had 15 devices that had not been classified as Critical Assets used in the access control and monitoring of its PSP. As a consequence of WECC_URE2's failure to properly identify the assets as PACM devices, the SME determined that WECC_URE2 failed to afford the 15 devices the protections required by CIP-006-1 R1.8, specifically the protections of CIP-005 R2, and R3; CIP-007 R1-R9; and CIP-009 R1-R5. The SME determined that the violation included 15 out of WECC_URE2's 22 PACM devices. WECC reviewed the Self-Certification and SME findings. Based on this review, WECC determined that WECC_URE2 is in violation of CIP-006-1 R1. Specifically, WECC determined that WECC_URE2 failed to afford the protections outlined in CIP-006-1 R 1.8, specifically the protections of CIP-005 R2 and R3; CIP-007 R1-R9; and CIP-009 R1-R5, to 15 PACM devices. WECC determined that the violation was a result of WECC_URE2's failure to properly identify the devices as Critical Assets used in the access control or monitoring of its PSPs. WECC determined that the PACM were not behind a firewall or other electronic perimeter. This was confirmed by checking individual asset, application, router and firewall configurations. The causes of the violation were that CIP roles and responsibilities were not understood by system operators, when the system was implemented it was not identified as being in scope, and the methodology to identify assets was not consistent between the groups managing components of PACM.	CIP-006-1	R1; R1.8	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
13	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC determined that the violation occurred over a period of approximately four years and included approximately 68% of WECC_URE2's PACM devices. WECC determined that, based on the duration and magnitude of WECC_URE2's failure, there was an increased opportunity for malicious cyber attacks to occur. Furthermore, WECC determined that WECC_URE2's failure created a situation where WECC_URE2 may have been unable to properly detect and prevent potential cyber attacks. Although WECC_URE2 failed to afford various protections required by CIP-006-1 R1 to 15 PACM devices, each of the devices is located on WECC_URE2's corporate network and is monitored 24 hours a day 7 days a week. Additionally, each of the devices has strong passwords that comply with additional CIP criteria. Finally, all of the devices reside within secure facilities where access is limited to employees who have undergone personnel risk assessments and have Critical Asset training.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
13	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Self-Certification	To mitigate this violation, WECC_URE2: 1) clarified CIP roles and responsibilities and provided training to management stakeholders on CIP-006 and refresher SME training for CIP compliance specific to CIP-006; 2) applied CIP controls to PACM and addressed system not being captured by making changes to the CIP review process and Cyber Vulnerability Assessment process to find unknown systems which may be in scope; 3) improved organizational continuity for demonstrating compliance by producing a set of procedures that show how to gather, maintain, store, and submit execution evidence for compliance activities; 4) developed a single methodology for identifying all Cyber Asset classes between all functional groups; 5) corrected network documentation and improved the documentation update process; and 6) provided focused awareness of interrelationships between CIP-005, CIP-006, and CIP-007 by providing refresher SME training for CIP compliance specific to CIP-006.	8/1/2013	9/23/2015

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
13	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
14	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014014018	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
14	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-007-1 R6. Specifically, WECC_URE2 reported that it failed to review logs of system events related to cyber security and maintain records documenting review of logs, as required by CIP-007 R6. While WECC_URE2 reported that log reviews were being conducted, evidence of the review was insufficient. Additionally, WECC_URE2 reported that there were insufficient procedures and internal controls to assure the log reviews were occurring and being documented in a way that demonstrates compliance with the Requirement. WECC reviewed the Self-Report at WECC_URE2's mock audit results. WECC reviewed the details of the Self-Report and issued data requests for additional information. Based on the review, WECC determined that WECC_URE2 failed to establish a method to document the review and handling of events related to cyber security. While the evidence reviewed confirmed that WECC_URE2 was logging security events related to cyber security and generating alerts to response personnel, WECC_URE2 had no process or evidence to demonstrate that the alerts were being reviewed. WECC determined that WECC_URE2 was in violation of CIP-007-1 R6 for failing to review logs of system events related to cyber security and maintain records documenting review of logs. The root cause was insufficient procedures and internal controls to assure the log reviews were occurring and being documented in a way which demonstrates compliance. The cause was an insufficient procedures and internal controls to assure the log reviews were occurring and being documented in a way which demonstrates compliance with the Requirement.	CIP-007-1	R6; R6.5	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
14	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE2's devices were generating alerts and the alerts were being reviewed; however, WECC_URE2 was not capturing any evidence of these reviews. Without the documentation, there is no assurance that these reviews were consistently occurring. Failing to review system events related to cyber security could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Nevertheless, WECC_URE2 implemented good preventive controls. Specifically, WECC_URE2 enabled logging and alerting on all devices where technically capable. WECC_URE2's alerts were configured in a manner to notify responsible personnel of any potential cyber security events on its system. Although WECC_URE2 was not documenting its review and handling of the events, it does appear its response personnel were receiving the alerts and training on properly responding to them, reducing the risk of an event going unnoticed and unchecked.	when the Standard became mandatory and enforceable on WECC_URE2	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
14	No penalty (for WECC200901795, WECC200901796, WECC201102961, WECC201102962, WECC201102963, WECC2013012054, and WECC2014014018)	Self-Report	To mitigate this violation, WECC_URE2 implemented a policy of log review and attestation of the review.	7/31/2014	11/19/2015

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
14	Agrees/Stipulates	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE2's compliance history in determining the disposition track. WECC considered WECC_URE2's compliance history to be an aggravating factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
15	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901552	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
15	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-007-1 R1. WECC_URE3 stated in its Self-Report that it failed to document cyber security testing as required by the Standard. WECC_URE3 is required to document testing in a manner that reflects the production environment under CIP-007-1 R1.2. WECC_URE3 is also required to document the results of its cyber security testing under CIP-007-1 R1.3. During an interview with WECC_URE3 personnel regarding this violation, a WECC subject matter expert (SME) confirmed that WECC_URE3 did not document any cyber security testing. Based on information from the Self-Report and the subsequent interview with WECC_URE3, WECC determined that WECC_URE3 had a violation of CIP-007-1 R1 because it failed to document its cyber security testing and results. WECC reviewed the Self-Report and the SME's findings and concluded that WECC_URE3 had a violation of CIP-007-1 R1 because WECC_URE3 failed to have test procedures covering new Cyber Assets as required by R1; failed to document that testing is being performed as required by R1.2; and failed to document test results as required by R1.3. Because the violation period of R1.1 found during the Spot Check coincides with the Self-Reported violations of R1.2 and R1.3, WECC processed this violation in conjunction with WECC200901713.	CIP-007-1	R1; R1.2; R1.3	Medium	Severe

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
15	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 failed to create or implement procedures for a range of equipment and significant changes to Cyber Assets as required by the Standard. However, WECC_URE3 described during a WECC interview that it was using subject expert experience and a security utility program to measure the effect of changes and test functionality on changes to its Supervisory Control and Data Acquisition (SCADA)/Automatic Generation Control (AGC) systems. Additionally, all testing was performed on a development system prior to installation on the production system in a manner that ensured the reliability of the online system remained intact	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
15	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Report	To mitigate this violation, WECC_URE3: 1) developed and implemented a SCADA Change Authorization Form; and 2) installed a software tool for detecting and reporting system changes.	7/30/2009	8/26/2009

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
15	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
16	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901626	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
16	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-007-1 R4. Supplemental information was provided during an interview with WECC_URE3 personnel. WECC_URE3 stated in its Self-Report that its anti-virus and malware prevention tools were not being applied to various Cyber Assets within its Electronic Security Perimeter (ESP). Because CIP-007-1 R4 requires that WECC_URE3 shall use anti-virus software and other malicious software prevention tools on all Cyber Assets, within the ESP, WECC_URE3 reported a violation of the Standard. WECC_URE3 did not have a properly working process for updating the anti-virus and malware prevention signatures on the platforms where they are installed and was in violation of CIP-007-1 R4.2. WECC reviewed the violation Self-Report and additional information and determined that WECC_URE3 failed to have an implemented process for using anti-virus software and other malware prevention on Cyber Assets within WECC_URE3's ESP. Specifically, WECC_URE3 identified it has an active platform where it demonstrated there was a technically feasible malware scanning solution. However, anti-virus software and other malware prevention tools had not been deployed on these platforms as required. Based on WECC_URE3's failure to deploy anti-virus software and other malware prevention tools, WECC determined that WECC_URE3 had a violation of CIP-007-1 R4. WECC reviewed the Self-Report and concluded that WECC_URE3 had a violation of the CIP-007-1 R4 because WECC_URE3 failed to use anti-virus software and other malicious software prevention tools on all Cyber Assets within the ESP as required by the Standard.	CIP-007-1	R4; R4.2	Medium	High

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
16	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. A failure to deploy anti-virus software on Cyber Assets within the ESP means an increased risk of exposure to malware. Although WECC_URE3 has mitigating controls to reduce the risk of external attacks, cyber incidents can originate from internal sources. Although insiders are not likely to have malicious intent, they may unintentionally plant malicious software by connecting infected systems or devices to an internal network resulting in a compromise of the integrity/confidentiality of the system or by affecting system performance, availability, and/or storage capacity. WECC_URE3 has highly-restrictive firewall rules in place that reduced the risk.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
16	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Report	To mitigate this violation, WECC_URE3 implemented anti-virus signature updating and system scanning to prevent viruses and malware on systems within the Supervisory Control and Data Acquisition (SCADA) ESP.	11/19/2009	12/9/2009

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
16	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
17	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901645	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-007-1 R3. WECC_URE3 stated in its Self-Report that it failed to document security patches and security upgrades to Cyber Assets within the Electronic Security Perimeter (ESP). WECC_URE3 reported a violation because it failed to document assessments within 30 calendar days as required by R3.1 and implementations as required by R3.2. During an internal review, WECC_URE3 discovered that it had not been following its configuration management process for security patches to Cyber Assets. Specifically, WECC_URE3 reported that it failed to document the process implementation, compensating measures to mitigate risks, or the acceptance of risk. The WECC_URE3 process states that security patch assessments must be documented within 30 calendar days, as required by CIP-007-1 R3.1. WECC_URE3 also reported that it failed to document the implementation of security patches as required by R3.2. Although WECC_URE3 had established and documented a security patch management program as required by CIP-007-1, the program had not been fully implemented. Based on information from the Self-Report and the subsequent interview with WECC_URE3, a WECC subject matter expert (SME) determined that WECC_URE3 had a violation because it failed to document security patches as required by CIP-007-1 R3.1, and failed to document the implementation of security patches to Cyber Assets within the ESP as required by R3.2. The WECC_URE3 process states that security patch assessments must be documented within 30 calendar days, as required. WECC_URE3 also reported that it failed to document the implementation of security patches as required by R3.2. WECC concluded that WECC_URE3 had a violation of CIP-007-1 R3 because WECC_URE3 failed to document the assessment of security patches as required by R3.1, or the implementation of security patches as required by R3.2. The cause was WECC_URE3 not following its procedure.	CIP-007-1	R3; R3.1; R3.2	Lower	High
17					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
17	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. A failure to document security changes to Critical Assets may result in an increased risk of a cyber attack on the assets. Although WECC_URE3 has mitigating controls to reduce the risk of external attacks, cyber incidents can originate from internal sources. Although insiders are not likely to have malicious intent, they may unintentionally plant malicious software by connecting infected systems or devices to an internal network resulting in a compromise of the integrity/confidentiality of the system or by affecting system performance, availability, and/or storage capacity. Although not fully implemented, WECC_URE3 had established and documented a security patch management program as required by CIP-007-1, which helped reduce the risk.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
17	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Report	To mitigate this violation, WECC_URE3 assessed patches, installed the patches where appropriate, and completed the documentation associated with the patches, for all Supervisory Control and Data Acquisition (SCADA) systems.	10/27/2009	10/28/2009

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
17	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. Although WECC_URE3 self-reported this violation, because it self-reported during the 60-day CIP Spot Check notification window, no Self-Report credit was applied. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
18	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901710	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	During a Spot Check WECC determined that WECC_URE3 was in violation of CIP-003-1 R1. WECC determined that the WECC_URE3 Cyber Security Policy failed to address three requirements in CIP-002 through CIP-009 as required by CIP-003-1 R1.1. WECC also determined that the WECC_URE3 Cyber Security Policy was not approved by the senior manager as required by CIP-003-1 R1.3. WECC notified WECC_URE3 at the time of the review that there was a violation of the Standard. During the Spot Check, WECC_URE3 presented a Program Cyber Security Plan (PCSP) as evidence of its compliance with CIP-003-1 R1. WECC reviewed the PCSP and determined it did not address CIP-002-1 R1, CIP-002-1 R2, and CIP-002-1 R4 as required by CIP-003-1 R1.1. Because CIP-003-1 R1.1 requires that an entity's Cyber Security Policy address each of the requirements in CIP-002 through CIP-009, WECC determined this was a violation of the Standard. WECC also determined that WECC_URE3's assigned senior manager had not approved the PCSP as required by CIP-003-1 R1.3. The WECC_URE3 PCSP's annual review and approval had actually been performed by the chief information officer, not the assigned senior manager. WECC_URE3 offered no evidence that the authority to conduct the annual review had been delegated. Because CIP-003-1 R1.3 requires that annual review and approval of the Cyber Security Policy be performed by the senior manager, WECC determined this was a violation of the Standard. WECC concluded that WECC_URE3 had a violation of CIP-003-1 R.1 because it failed to address all CIP standards in its Cyber Security Policy as required by R1.1, and also failed to have the assigned senior manager approved the plan as required R1.3.	CIP-003-1	R1; R1.1; R1.3	Medium	Severe
18					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
18	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although WECC_URE3 failed to address three CIP-002 requirements in its Cyber Security Policy, it was found to be compliant with the individual standards. Furthermore, although a WECC_URE3 senior manager did not approve the PCSP, it was approved and reviewed at a high level within the organization. This approval is a good indication of WECC_URE3 management's commitment to the PCSP.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
18	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Spot Check	To mitigate this violation, WECC_URE3: 1) updated its Cyber Security Policy to be compliant with CIP-002 through CIP-009; and 2) submitted evidence that the Cyber Security Policy was approved by the designated senior manager.	9/1/2009	7/30/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
18	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
19	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901711	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
19	During a Spot Check WECC determined that WECC_URE3 was in violation of CIP-004-1 R2. During the Spot Check, WECC_URE3 identified a Program Cyber Security Plan (PCSP) as its cyber security training, to demonstrate compliance with CIP-004-1 R.2. The entity provided two annual versions of the document. WECC determined that the PCSP had not been annually reviewed as required by CIP-004-1 R2, as it was last updated in more than a year prior. WECC_URE3 offered no evidence that the PCSP had been reviewed or updated since its introduction. Because the Standard requires that an annual review be conducted on the cyber security training program, WECC determined this was a violation of CIP-004-1 R2 because WECC_URE3 did not review and update its cyber security training materials annually. WECC concluded that WECC_URE3 had a violation of CIP-004-1 R2 because WECC_URE3 failed to review and update its cyber security training materials as required by CIP-004-1 R2.	CIP-004-1	R2	Lower	High

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
19	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this violation, WECC_URE3 failed to annually review the plan as required. Although WECC_URE3 failed to have a documented cyber security training program, it had provided training to all individuals with access to Critical Cyber Assets on the prior version of the PCSP.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
19	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Spot Check	To mitigate this violation, WECC_URE3 updated its Cyber Security Policy. The new document was reviewed and approved by WECC_URE3's then interim designated senior manager.	9/1/2009	9/3/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
19	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
20	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901712	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	During a Spot Check WECC determined that WECC_URE3 was in violation of CIP-004-1 R4. WECC determined that WECC_URE3 failed to maintain lists of individuals with administrative access to Critical Cyber Assets as required by CIP-004-1 R4. WECC_URE3 also failed to perform quarterly reviews of its access lists as required by CIP-004-1 R4.1. WECC notified WECC_URE3 at the time of the Spot Check review that there was a possible violation of CIP-004-1 R4. During the Spot Check, WECC_URE3 provided WECC with several lists detailing individuals with access to WECC_URE3's Critical Cyber Assets (CCAs). After reviewing the documents, WECC determined that WECC_URE3 had failed to maintain a list of individuals with administrative access to CCAs. WECC_URE3 confirmed that there were two individuals with administrative access that did not appear on the presented lists. WECC_URE3's response to a WECC Spot Check data request provided no additional evidence of the missing access lists or proof that the network personnel access file had been reviewed as required. Because CIP-004-1 requires that WECC_URE3 maintain lists of all personnel with access to CCAs, WECC determined this was a violation of the CIP-004-1 R4. Additionally, WECC established that WECC_URE3 had not performed quarterly reviews of all access lists. Specifically, WECC_URE3 had not reviewed its document that details the individuals with access to network equipment with the WECC_URE3 Electronic Security Perimeter (ESP). As evidence of compliance, the entity provided a document which discusses and documents its quarterly reviews of access lists. The document showed a reviewer name for two quarters, however it did not have a specific date of review. Because the review dates could not be confirmed, WECC determined this was a violation of the Standard. WECC concluded that WECC_URE3 had a violation of the CIP-004-1 R4 because WECC_URE3 failed to maintain a list of all individuals with access to Critical Cyber Assets as required by R4 and also failed to perform quarterly reviews of those lists as required CIP-004-1 R4.1.	CIP-004-1	R4; R4.1	Lower	Severe
20					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
20	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. A failure to maintain lists of those with access to CCAs could result in individuals having unnecessary access to systems. Such access could potentially be misused to perform unauthorized actions on CCAs, possibly affecting the Bulk Electric System. In this situation, WECC_URE3 has strong physical access controls to control access to its CCAs. Furthermore, WECC_URE3 does not allow remote access to its CCAs from outside the Physical Security Perimeter.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
20	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Spot Check	To mitigate this violation, WECC_URE3: 1) reviewed the Supervisory Control and Data Acquisition (SCADA) access list and has continued to do quarterly reviews; 2) performed analysis to identify issues in the access list control; 3) identified possible solutions to eliminate gaps in the processes; and 4) implemented a document management system which includes alerts for document review.	6/30/2009	8/25/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
20	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
21	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC200901713	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
21	During a Spot Check WECC determined that WECC_URE3 was in violation of CIP-007-1 R1. WECC determined that WECC_URE3 failed to create cyber security test procedures as required by R1.1. WECC_URE3 provided its supervisory control data acquisition form and a security change control process documents as evidence of WECC_URE3 test procedures. WECC found that WECC_URE3's test procedures did not cover new Cyber Assets; it only covered patches to WECC_URE3's Critical Cyber Assets (CCAs) within its Electronic Security Perimeter (ESP). WECC also found that WECC_URE3 did not have procedures in place that address significant changes in all Cyber Assets within the ESP, only its CCAs. Based on the procedures presented by WECC_URE3, WECC concluded that WECC_URE3 had a violation of R1.1. WECC concluded that WECC_URE3 had a violation of CIP-007-1 R1 because WECC_URE3 failed to create cyber security test procedures for significant changes to all Cyber Assets as required by R1.1. Because the violation period of R1.1 found during the Spot Check coincides with the Self-Reported violations of R1.2 and R1.3, WECC processed this violation in conjunction with WECC200901552.	CIP-007-1	R1.1	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
21	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 failed to create or implement procedures for a range of equipment and significant changes to cyber assets as required by the Standard. However, WECC_URE3 described during a WECC interview that it was using subject expert experience and a security utility program to measure the effect of changes and test functionality on changes to its SCADA/Automatic Generation Control (AGC) systems. Additionally, all testing was performed on a development system prior to installation on the production system in a manner that ensured the reliability of the online system remained intact.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
21	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Spot Check	To mitigate this violation, WECC_URE3: 1) performed gap analysis of documentation and evidence; 2) confirmed base configuration documentation to establish similarities between production and development environments utilizing existing tool; and 3) confirmed procedures are developed to ensure a direct mapping between execution evidence and the cyber controls tests.	6/17/2010	9/1/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
21	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
22	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201002235	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-004-1 R4. A WECC subject matter expert (SME) reviewed the Self-Report and conducted a telephone interview with WECC_URE3 personnel. The SME determined an individual with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) retired. The individual was an employee of a company that WECC_URE3 had a Joint Use Agreement with. The other company did not inform WECC_URE3 of the retirement in a timely manner. The SME determined WECC_URE3 should have revoked access rights for this individual within seven calendar days of the employee's retirement. Based on the interview and the Self-Report, the SME determined WECC_URE3 did not revoke this individual's access in a timely manner and thus determined WECC_URE3 had a violation of CIP-004-1 R4.2. The SME further determined WECC_URE3 did not quarterly review its lists of its personnel who have access to CCAs, and update the lists within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel. Therefore, the SME determined WECC_URE3 had a violation of CIP-004-1 R4.1. WECC determined that WECC_URE3 did not conduct quarterly review of its lists of personnel with authorized cyber or authorized unescorted physical access to CCAs or update its lists within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel. WECC further determined WECC_URE3 failed to revoke access to CCAs within seven calendar days for personnel who no longer require such access to CCAs. Therefore, WECC determined WECC_URE3 has a violation of CIP-004-1 R4, specifically R4.1 and R4.2.	CIP-004-1	R4; R4.1; R4.2	Medium	Severe
22					

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
22	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 did not review the lists of its personnel who have access to CCAs quarterly and update the lists within seven calendar days of any change of personnel with such access to CCAs, nor did it revoke such access within seven days. Such a failure could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to CCAs essential to the operation of the Bulk Electric System (BES), thereby potentially negatively impacting the BES. However, in this case, the violation relates to WECC_URE3's failure to revoke access within seven days of an employee retiring. During the individual's time as a WECC_URE3 employee, the individual appropriately had authorized access to CCAs. Further, as a compensating measure, WECC_URE3 maintains manual logging of physical access of personnel entering and exiting its facilities.	seven calendar days after the personnel no longer required such access	Mitigation Plan completion

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
22	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Report	To mitigate this violation, WECC_URE3 removed all Joint User Agreement company employees' access in the access control system, until it could be confirmed the company employees understood the requirements and retook the cyber security training.	8/23/2010	6/2/2011

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
22	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's CIP-004 R4 compliance history to be an aggravating factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
23	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201002237	Settlement Agreement
24	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201002238	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
23	WECC_URE3 submitted a Self-Certification stating that it was in violation of CIP-007-1 R2. A WECC subject matter expert (SME) reviewed the Self-Certification and conducted a telephone interview with WECC_URE3 personnel. The SME determined two PCs at WECC_URE3's substation did not have a record of ports and services being evaluated and disabled, and therefore WECC_URE3 did not establish and document a process to ensure that only ports and services required for normal and emergency operations are enabled. The SME determined the two PCs are connected to WECC_URE3's Electronic Security Perimeter (ESP). WECC_URE3 classified these PCs as Critical Cyber Assets (CCAs). Thus, the SME determined WECC_URE3 had a violation of CIP-007-1 R2. WECC determined that WECC_URE3's failure to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled on the two PCs is a violation of CIP-007-1 R2.	CIP-007-1	R2	Medium	Severe
24	WECC_URE3 submitted a Self-Certification stating that it was in violation of CIP-007-1 R3. A WECC subject matter expert (SME) determined two PCs at WECC_URE3's substation did not have a record of an assessment for implementation of security patches. The SME determined the two PCs are connected to WECC_URE3's Electronic Security Perimeter (ESP). WECC_URE3 classified these PCs as Critical Cyber Assets (CCAs). The SME determined WECC_URE3 did not document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades and failed to document the implementation of security patches for the PCs. Thus, the SME determined WECC_URE3 had a violation of CIP-007-1 R3. WECC determined that WECC_URE3's failure to document its assessment of security patches and security upgrades for applicability to the two PCs within 30 calendar days of the patches or upgrades being made available is a violation of CIP-007-1 R3.	CIP-007-1	R3	Lower	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
23	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 did not ensure that only those ports and services required for normal and emergency operations are enabled for two PCs. A failure to ensure that only those ports and services required for normal and emergency operations are enabled poses significant risk to the entity's Cyber Assets by potentially allowing for unauthorized internal or external access, which could allow for successful cyber attacks against CCAs essential to operation of the Bulk Electric System. However, as compensating measures, WECC_URE3 stated that it implemented controls to log and monitor access to CCAs within the ESP within which the two PCs reside. In addition, the access point to this ESP only allows access to the ports and services necessary for normal operations. Further, the violation is limited to two legacy PCs within WECC_URE3's system.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion
24	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 failed to assess security patches and upgrades for two PCs. A failure to assess security patches could result in vulnerabilities remaining unaddressed for extended periods of time. This increases the risk of a successful cyber attack against CCAs essential to the operation of the Bulk Electric System. As a compensating measure, WECC_URE3 personnel stated that all other devices on the applicable network are current on patches pursuant to WECC_URE3's security patch management plan. In addition, WECC_URE3 implemented controls to log and monitor access to CCAs within the ESP in scope.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
23	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Certification	To mitigate this violation, WECC_URE3: 1) removed the devices from the network and had the network administrator verify disconnection; and 2) ensured future Cyber Assets, if connected to the network, will utilize a current operating system and not a legacy operating system.	2/2/2010	10/20/2010
24	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Certification	To mitigate this violation, WECC_URE3: 1) removed the devices from the network and had the network administrator verify disconnection; and 2) ensured future Cyber Assets, if connected to the network, will utilize a current operating system and not a legacy operating system.	2/2/2010	10/20/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
23	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.
24	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3’s CIP-007 R3 compliance history to be an aggravating factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
25	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201002239	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
25	WECC_URE3 submitted a Self-Certification stating that it was in violation of CIP-007-1 R4. A WECC subject matter expert (SME) determined WECC_URE3 did not use anti-virus software and other malicious software malware prevention tools on two PCs at WECC_URE3's substation. The SME determined the two PCs are connected to WECC_URE3's Electronic Security Perimeter (ESP). WECC_URE3 classified these PCs as Critical Cyber Assets (CCAs). The SME determined WECC_URE3 did not use anti-virus software and other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within its ESP. Thus, the SME determined WECC_URE3 had a violation of CIP-007-1 R4. WECC determined that WECC_URE3's failure to use anti-virus software and other malicious software prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on the two PCs within its ESP is a violation of CIP-007-1 R4.	CIP-007-1	R4	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
25	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 did not use anti-virus software and other malicious software (malware) prevention tools for its Cyber Assets, on two PCs. Failure to do so could allow existing or new malicious software, originating from, e.g., a security patch, service pack, vendor release, application or database update, to be introduced to the Cyber Assets, thereby exposing cyber security vulnerabilities into the CCAs. If exposed, such vulnerabilities could negatively affect the normal operation of the Bulk Electric System. As a compensating measure, WECC_URE3 installed anti-virus and other malicious software prevention tools on all other capable devices on the network in scope. In addition, WECC_URE3 personnel stated that WECC_URE3 implemented controls to log and monitor access to CCAs within the ESP in scope.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
25	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Certification	To mitigate this violation, WECC_URE3: 1) removed the devices from the network and had the network administrator verify disconnection; and 2) ensured future Cyber Assets, if connected to the network, will utilize a current operating system and not a legacy operating system.	2/2/2010	10/20/2010

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
25	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
26	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2012009538	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
26	WECC_URE3 submitted a Self-Certification stating that it was in violation of CIP-007-1 R4. A WECC subject matter expert (SME) contacted WECC_URE3 to discuss its self-certification. According to the WECC SME, WECC_URE3 stated that it failed to rename default administrator accounts on ten devices prior to putting them into production. All ten devices are Critical Cyber Assets (CCAs). Nine of the devices are used to collect data such as power voltage status, circuit breaker status and alarms, from protective relays and transmit that data to Remote Terminal Units (RTU). One of the devices involved in this violation is an RTU that controls physical equipment in substations. The WECC SME concluded that WECC_URE3 was in violation of CIP-007-1 R5.2.1. WECC reviewed WECC_URE3's Self-Certification and determined that WECC_URE3 is in violation of CIP-007-1 R5.2.1 for failing to rename default administrator accounts on ten CCAs prior to putting them into production. WECC_URE3 did not include the removal, disabling, or renaming of such accounts where possible, for accounts that must remain enabled, passwords were changed prior to putting any system into service. The cause of this finding was due to the misinterpretation of CIP-007-R5. Prior to this finding during the WECC_URE3 Self-Certification for 2011, it was the general understanding that WECC_URE3 met compliance for CIP-007-R5.2.1 on the device by controlling access authentication through technical and procedural controls.	CIP-007-1	R5.2.1	Medium	High

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
26	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to rename default administrator accounts prior to putting them into service could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to CCAs essential to the operation of the Bulk Electric System (BES), thereby potentially negatively affecting the BES. These devices are located at various substations inside Electronic Security Perimeters and Physical Security Perimeters. As compensating measures, WECC_URE3 stated that the default administrator accounts passwords were changed annually, met the CIP-007 R5.3 complexity requirements, were changed when there were personnel changes, and access to the devices required multi-factor authentication. In addition, all personnel with access to the accounts had current CIP training and personnel risk assessments and the devices were monitored continuously for physical and cyber access and account access was reviewed quarterly.	when the Standard became mandatory and enforceable on WECC_URE3	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
26	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Certification	To mitigate this violation, WECC_URE3: 1) contacted engineering labs to confirm administrator accounts could be changed and requested information about how to proceed; 2) tested the process for changing administer accounts; 3) renamed the default administrator accounts; and 4) communicated the details of the violation at the Annual Maintenance and Engineering Meeting to develop a common understanding of the NERC requirement and the need to rename administrator accounts on CCAs prior to putting them into service.	3/14/2012	8/30/2012

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
26	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's compliance history and determined there were no relevant instances of noncompliance.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
27	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2012010260	Settlement Agreement

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
27	WECC_URE3 submitted a Self-Report stating that it was in violation of CIP-002-2 R3. A WECC subject matter expert (SME) contacted WECC_URE3 to discuss its Self-Report. According to the WECC SME, WECC_URE3 stated that it failed to identify one of its Critical Cyber Assets (CCAs). The CCA WECC_URE3 failed to identify is a laptop used to periodically conduct Cyber Vulnerability Assessments (CVA) on WECC_URE3's Electronic Security Perimeters (ESPs). The laptop involved met WECC_URE3's CCA criteria and should have been added to its CCA list when it was put into service. The WECC SME concluded that WECC_URE3 was in violation of CIP-002-2 R3. WECC determined that WECC_URE3 is in violation of CIP-002-2 R3 for failing to identify one of its devices as a CCA. The root cause was that the laptop was connected to the Supervisory Control and Data Acquisition (SCADA) ESP in order to conduct CVA scans and was not considered a potential CCA due to its temporary connection to the ESP. At the time the laptop was put into service, there was not a documented methodology for CCA determination. The only determination criteria in the past was if the Cyber Asset was in an ESP then it was considered a CCA and temporary devices were not considered in the process and the laptop was excluded.	CIP-002-2	R3	High	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
27	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Failure to identify CCAs could result in leaving CCAs unprotected and vulnerable to a cyber threat, and could pose a risk to the associated Critical Asset. This can negatively impact the operation of the Bulk Electric System. In this instance, WECC_URE3 failed to identify one CCA that met its criteria for a CCA and was not added to its CCA list. The device in scope was a laptop used to conduct CVAs. The device was routinely added and removed from all of the entity's ESPs to conduct these periodic CVAs. As this was a laptop used on different ESPs in different physical locations, WECC_URE3 cannot ensure this device was inside an identified Physical Security Perimeter (PSP) at all times. As compensating measures, WECC_URE3 stated that only one individual had access to the device, it was only added to an ESP when it was conducting a CVA, and it was only used on designated ESPs and, thus when in service, was always in a protected network behind restrictive firewalls, and implemented AV/Malware prevention tools. WECC_URE3 also stated that although the device was mobile, while it was connected to an ESP it was in an identified and protected PSP. Finally, WECC_URE3 stated that the device in scope would no longer be considered a CCA using WECC_URE3's current CCA identification methodology.	when the device involved was put into service	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
27	No penalty (for WECC200901552, WECC200901626, WECC200901645, WECC200901710, WECC200901711, WECC200901712, WECC200901713, WECC201002235, WECC201002237, WECC201002238, WECC201002239, WECC2012009538, WECC2012010260)	Self-Report	To mitigate this violation, WECC_URE3: 1) implemented a methodology for determining CCAs; and 2) provided on the job training on the use of this new methodology and specifically temporary devices.	4/11/2012	10/25/2012

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
27	Agrees/Stipulates	WECC reviewed WECC_URE3's internal compliance program (ICP) and considered it to be a factor in the disposition determination. WECC considered WECC_URE3's CIP-002 R3 compliance history to be an aggravating factor in the disposition determination.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
28	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2015014880	Settlement Agreement

	F	G	H	I	J
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
28	WECC_URE4 submitted a Self-Report and approximately a month later WECC_URE4 submitted a Self-Certification stating that it was in violation of CIP-006-1 R3. WECC_URE4 identified the noncompliance during a mock audit. WECC_URE4 reported that it failed to implement appropriate technical and procedural controls per CIP-006-1 R3 guidelines. WECC reviewed the Self-Certification information and determined that WECC_URE4 failed to implement appropriate technical and procedural controls for monitoring physical access at two emergency/service doors to a Physical Security Perimeter (PSP) for twenty-four hours a day, seven days a week. The two PSP access points did not incorporate card readers and are identified as the emergency/service exit doors. Both are secured using mechanical hardware with magnetic door contacts monitored twenty-four hours a day, seven days a week remotely by the contracted security guards via intrusion monitoring software. However, when the first authorized personnel enters the PSP, he or she disables the alarm system, which disables the control room motion detection devices and the magnetic door contacts on the service doors. This allows additional authorized personnel to unlock the dead bolt with a key and enter the PSP through the service doors without any logging and/or triggering an alarm if the door is left open, since the motion detectors are disabled when the control room is occupied. WECC determined that WECC_URE4 is in violation of CIP-006-1 R3 for failing to implement appropriate technical and procedural controls for monitoring physical access to a PSP. The root cause of the violation was a lack of compliance understanding. The system was set up prior to the existence of the CIP standards and WECC_URE4 did not believe it was an issue when the CIP standards became enforceable.	CIP-006-1	R3	Medium	Severe

	K	L	M
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**
28	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE4 failed to implement appropriate technical and procedural controls for monitoring physical access at two emergency/service doors to a PSP twenty-four hours a day, seven days a week. Failing to implement technical and procedural controls for monitoring physical access at two emergency/service doors could allow unauthorized personnel access to the PSP. If the Physical Access Control System (PACS) would have been disarmed and the mechanical key lock defeated, unauthorized personnel would have access to several 230 kV transmission lines and the bus tie breaker between WECC_URE4 and a neighboring entity. WECC_URE4 implemented a dead bolt lock that restricted physical access to the PSP and a seven foot fence with barbed wire to prevent unauthorized physical access to the substation, as preventive controls. As an additional preventive control, the keys used to open the dead bolt locks are assigned to numerous individuals. Keys are accounted for using a key log and no one can access the two service doors without a key. WECC_URE4 also implemented good detective controls. Specifically, WECC_URE4 has employees who are working inside the PSP during normal business hours, and a guard monitors the two service doors via closed-circuit television cameras during non-business hours. Together, these employees would detect if someone attempted to physically damage the devices. Additionally, as revealed by an engineering study, loss of the transmission lines and tie-breaker from the substation in scope would not cause an overload or excessive voltage deviation.	when the Standard became mandatory and enforceable for WECC_URE4	Mitigation Plan completion

	N	O	P	Q	R
1	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
28	No penalty	Self-Certification	To mitigate this violation, WECC_URE4: 1) removed the doors from the PACS, so the alarms will now alert when doors are open and will be monitored by a guard twenty-four hours a day, seven days a week; 2) installed an audible alarm on the exterior of the control room that must be silenced and reset over the alarm monitoring software from the twenty-four hours a day, seven days a week, guard office; and 3) updated its procedures and added signage to require personnel to call security before using either service door.	11/12/2014	8/14/2015

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
28	Agrees/Stipulates	WECC reviewed WECC_URE4's internal compliance program (ICP) and considered it to be a mitigating factor in the disposition determination. WECC_URE4 did not receive mitigating credit for self-reporting because the Self-Report was submitted during the self-certification period.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 29, 2016

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of violations of Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

During the early stages of utilities becoming compliant with NERC Reliability Standards, URE submitted a Self-Certification for 36 CIP violations. At the time, URE stated that the entity's cyber security protections did not comply with NERC Reliability Standards, though cyber security protections were in place using government-issued guidelines.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002156	CIP-007-1	R1	Medium/ Severe	SC	Moderate	No Penalty
WECC201002157	CIP-007-1	R2	Medium/ Severe			
WECC201002158	CIP-007-1	R3	Lower/ Severe			
WECC201002159	CIP-007-1	R4	Medium/ Severe			
WECC201002160	CIP-007-1	R5	Medium/ Severe			
WECC201002161	CIP-007-1	R6	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002162	CIP-007-1	R7	Lower/ Severe	SC	Moderate	No Penalty
WECC201002163	CIP-007-1	R8	Lower/ Severe			
WECC201002164	CIP-007-1	R9	Lower/ Severe			
WECC201002166	CIP-006-1	R5	Medium/ Severe			
WECC201002169	CIP-006-1	R6	Medium/ Severe			
WECC201002170	CIP-003-1	R4	Medium/ Severe			
WECC201002171	CIP-003-1	R5	Lower/ Severe			
WECC201002172	ClP-003-1	R6	Lower/ Severe			
WECC201002173	CIP-008-1	R1	Lower/ Severe			
WECC201002174	CIP-008-1	R2	Lower/ Severe			
WECC201002176	CIP-004-1	R1	Lower/ Severe			
WECC201002177	CIP-004-1	R2	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002178	CIP-004-1	R3	Medium/ Severe	SC	Moderate	No Penalty
WECC201002179	CIP-004-1	R4	Medium/ Severe			
WECC201002180	CIP-009-1	R1	Medium/ Severe			
WECC201002181	CIP-009-1	R2	Medium/ Severe			
WECC201002182	CIP-009-1	R3	Lower/ Severe			
WECC201002183	CIP-009-1	R4	Lower/ Severe			
WECC201002184	CIP-009-1	R5	Lower/ Severe			
WECC201002186	CIP-005-1	R1	Medium/ Severe			
WECC201002187	CIP-005-1	R2	Medium/ Severe			
WECC201002188	CIP-005-1	R3	Medium/ Severe			
WECC201002189	CIP-005-1	R4	Medium/ Severe			
WECC201002190	CIP-005-1	R5	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002198	CIP-003-1	R1	Medium/ Severe	SC	Moderate	No Penalty
WECC201002199	CIP-003-1	R3	Lower/ Severe			
WECC201002200	CIP-006-1	R1	Medium/ Severe			
WECC201002201	CIP-006-1	R2	Medium/ Severe			
WECC201002202	CIP-006-1	R3	Medium/ Severe			
WECC201002203	CIP-006-1	R4	Medium/ Severe			

Common Risk Statement for all Violations

WECC determined that each of these violations posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE had not implemented all processes to become compliant with CIP standards and requirements, WECC confirmed that URE had implemented cyber security practices, procedures, and technologies different than those prescribed by NERC Reliability Standards CIP-002-009. For this reason, the risk posed by URE's violations was somewhat reduced.

Common Duration for all Violations

WECC determined the duration of the violations to be from the date when each Reliability Standard became mandatory and enforceable, through when URE completed its associated Mitigation Plan.

Common Certification and Verification Information for all Violations

URE certified that it had completed each Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002156 CIP-007-1 R1 - OVERVIEW

WECC determined that URE did not create or implement cyber security test procedures as required by CIP-007-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify test procedures for any assets that are now identified as Critical Cyber Assets (CCAs) pursuant to CIP-002 R3, that may assist in the development of NERC CIP test procedures and identified baseline security configurations;
2. ensure that test procedures to determine changes in baseline security configurations for each CCA and Cyber Asset located within an Electronic Security Perimeter (ESP) have been developed and documented;
3. ensure that the test procedures developed only validate the minimal ports and services necessary for normal and emergency operations remain enabled; and
4. ensure that a formal tracking capability exists to log the execution of test procedures, successful or failed tests, and any necessary test procedure updates or revisions resulting from test execution.

WECC201002157 CIP-007-1 R2- OVERVIEW

WECC determined that URE did not establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled as required by CIP-007-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing baseline configurations for all assets identified as CCAs pursuant to CIP-002 R3, and verify that the minimal ports and services have been determined for each Cyber Asset accordingly. Also, identify any procedures or other resources utilized to determine the minimal ports and services for each Cyber Asset that may assist in compliance with NERC CIP requirements for minimal ports and services;

2. ensure that the minimal ports and services for each CCA and Cyber Asset within the ESP have been established and documented; and
3. develop, document, and promulgate procedures to ensure that the minimal ports and services are enabled for each CCA and Cyber Asset prior to placement into an operational system.

WECC201002158 CIP-007-1 R2 - OVERVIEW

WECC determined that URE did not establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESPs as required by CIP-007-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing patch management processes and procedures that have been afforded to any Cyber Asset that is now identified as a CCA pursuant to CIP-002 R3, that may assist in the development of patch management procedures needed to comply with NERC CIP requirements;
2. implement a cyber security patch management procedure for tracking, evaluating, testing, and installing applicable security patches for all Cyber Assets within an ESP;
3. identify and document a monitoring capability that tracks the release of security updates, patches, vulnerabilities, and vendor notifications for all CCAs and Cyber Assets located within an ESP;
4. ensure that an assessment for applicability of a security patch or upgrade is conducted within 30 days of its availability;
5. ensure that all applicable security patches and upgrades are implemented pursuant to requirements and procedures identified in URE's NERC CIP cyber security policy; and
6. document the compensating measures applied to mitigate the risk of exposure for those patches and upgrades not feasible.

WECC201002159 CIP-007-1 R4 - OVERVIEW

WECC determined that URE did not use antivirus software and other malicious software (malware) prevention tools to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all of its Cyber Assets within the ESP as required by CIP-007-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. determine and document the type of existing antivirus and malware prevention tools required for all Cyber Assets now classified as CCAs or other non-critical Cyber Assets located within a defined ESP;
2. implement the antivirus and malware prevention tools as required based on assessment for all CCAs and Cyber Assets within an ESP;
3. document the approved Technical Feasibility Exception (TFE), where antivirus and malware prevention tools cannot be implemented due to technical limitations;
4. document any compensating measures applied to mitigate the risk of exposure, where TFEs are documented; and
5. establish and document the antivirus and malware prevention tool update process and supporting procedures.

WECC201002160 CIP-007-1 R5 - OVERVIEW

WECC determined that URE did not establish and enforce access authentication of and accountability for all user activity to minimize risk of unauthorized system access as required by CIP-007-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and review any documented authorizations for logical access to Cyber Assets that are now identified as CCAs pursuant to CIP-002 R3. This list will be a basis for personnel lists developed to comply with NERC CIP requirements;
2. implement and/or verify all individual and shared accounts, from the list of individuals with approved authorizations for electronic access and associate privileges;
3. develop and document all technical and operational controls that enforce access authorizations and accountability for user activity;
4. develop and implement procedures to ensure that all user and shared accounts are supported by management authorizations and support a valid "need to know";
5. develop and implement procedures to ensure that all user accounts approved by management are consistent with CIP-003 R5.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

WECC201002161 CIP-007-1 R6 - OVERVIEW

WECC determined that URE did not ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security as required by CIP-007-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify existing security status monitoring capabilities being performed for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the compliance with NERC CIP requirements for CIP-006 R6;
2. determine the scope of Cyber Assets that require security status monitoring, pursuant to the ESPs and hosted CCAs and Cyber Assets determined in CIP-005 R1;
3. design, implement, and document a security status monitoring capability for CCAs and Cyber Assets within the ESP;
4. design, implement, and document the technical and operational procedural mechanism for monitoring and identifying security in support of the security status monitoring capability; and
5. design, implement, and document the security status alerting capability related to the technical and/or operational mechanism implemented.

WECC201002162 CIP-007-1 R7 - OVERVIEW

WECC determined that URE did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP(s) as identified and documented in Standard CIP-005, as required by CIP-007-1 R7.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. design, implement, and document procedures to ensure that all data storage media is destroyed or erased from CCAs and Cyber Assets as part of a disposal process;
2. design, implement, and document procedures to ensure that data storage media has been erased prior to redeployment of any CCA or Cyber Asset within an ESP; and

3. promulgate the process that ensures the documentation of all CCA and Cyber Asset disposal and redeployment activities.

WECC201002163 CIP-007-1 R8 - OVERVIEW

WECC determined that URE did not perform a cyber vulnerability assessment of all Cyber Assets within the ESP as required by CIP-007-1 R8.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify the type, scope, and test results for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the development of test procedures and addressing of any identified vulnerabilities, or testing for minimal ports and services;
2. develop and promulgate the CIP vulnerability assessment procedures;
3. develop, execute, and document the results of the execution of the procedures for each identified and discovered Cyber Asset; and
4. prepare a mitigation plan addressing the correction of vulnerabilities identified.

WECC201002164 CIP-007-1 R9 - OVERVIEW

WECC determined that URE did not create the documentation required by CIP-007-1; therefore, it could not review and update the documentation as required by CIP-007-1 R9.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing system security, contingency, and recovery plans to identify documentation for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the compliance with NERC CIP requirements for CIP-007 R9;
2. identify and place documentation artifacts under management control, including guidance documents, process documents, configuration documents, and event documentation; and
3. develop a process to review all documentation, as part of ongoing maintenance processes annually at a minimum or within 30 days of a change required to support CIP-007 requirements.

WECC201002166 CIP-006-1 R5 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to retain physical access logs as required under CIP-006-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the physical access monitoring requirements in CIP-006 R5 and identify the type of monitoring implemented at all access points;
2. ensure that the physical security plans address and include operational and procedural controls to manage physical access 24 hours a day, seven days a week; and
3. implement the procedural control to monitor physical access identified in the physical security plan.

WECC201002169 CIP-006-1 R6 - OVERVIEW

WECC determined that URE did not implement a maintenance and testing program to ensure that all physical security systems function properly as required under CIP-006-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the Logging of Physical Access requirements in CIP-006 R6 and identify the type of logging or recording implemented;
2. ensure that the physical security plans address and include operational and procedural controls to manage physical access logging 24 hours a day, seven days a week; and
3. implement the physical access logging capabilities and methods identified in the physical security plan.

WECC201002170 CIP-003-1 R4 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy, pursuant to CIP-003-1. Instead, for the protection of CCAs, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document or implement a program to identify, classify, and protect information associated with CCAs as required by CIP-003-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. implement and document a process with supporting procedures to identify, classify, and protect CCA information as defined by CIP-003, R4.1;
2. develop a process and related procedures to execute an annual assessment and review to ensure compliance with CIP-003 R4.1 and classification pursuant to R4.2; and
3. develop a process and related procedures as part of an action plan that tracks the remediation of any identified deficiencies resulting from the assessment identified in Step 2 and pursuant to R4.3.

WECC201002171 CIP-003-1 R5- OVERVIEW

WECC determined that URE did not document or implement a program for managing access to protected CCA information as required by CIP-003-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. create, update, and maintain a list of assigned information control personnel and their scope of responsibilities pursuant to CIP-003 R5.1 and R5.1.1;
2. document a process and/or procedure to verify that the list of assigned information control personnel and their scope of responsibilities and associated access privileges are correct, correspond to industry needs, and identify appropriate roles and responsibilities; and
3. document a process and/or procedures to ensure that the verification process is executed on an annual basis and the results are documented accordingly.

WECC201002172 CIP-003-1 R6 - OVERVIEW

WECC determined that URE did not document or establish a process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software, and did not implement supporting configuration management activities to identify, control, and document all entity- or vendor-related changes to hardware and software components of CCAs, as required by CIP-003-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify existing configuration management plans (CMPs) where CCAs are included as "configuration items" and formally placed under control of the associated CMP;
2. update and revise the CMP, to identify any configuration items that are defined as CCAs pursuant to CIP-002 R3, and any additional CCAs that may not have been included within the existing CMP that should be included based on NERC CIP requirements outlined in CIP-002 R3.1-R3.3, CIP-005 R1, and CIP-006 R1;
3. update and revise the CMP (including any associated processes, procedures, or documentation) so that all CCAs are identified as such and formally communicate the revisions as part of the change control board's review and approval processes; and
4. maintain all documentation related to this Mitigation Plan as evidence of compliance.

WECC201002173 CIP-008-1 R1 - OVERVIEW

WECC determined that URE did not define methods, processes, and procedures for securing CCAs and non-critical Cyber Assets. Specifically, URE failed to develop and maintain a Cyber Security Incident response plan as required by CIP-008-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. expand or amend the current incident response procedures to ensure that they address various supervisory control and data acquisition installation-type incidents and events and developed procedures for reporting to ES-ISAC;
2. review and revise procedures as necessary to be consistent with URE's requirements for CIP-001 sabotage reporting;
3. review and revise procedures as necessary to be consistent with URE's power resources office, facilities instructions, standards, and techniques;
4. promulgate the revised procedures and establish/identify organizational parties who will have responsibility for incident command reporting/communication reporting, incident control, incident investigation, and resumption of normal operations; and
5. establish and implement a reminder solution for a test of the incident response procedures and plan at least once each year.

WECC201002174 CIP-008-1 R2 - OVERVIEW

WECC determined that URE did not define methods, processes, and procedures for securing CCAs and non-critical Cyber Assets. Specifically, URE failed to retain relevant documentation related to Cyber Security Incidents as required by CIP-008-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to establish and implement a central incident reporting repository for three years of records.

WECC201002176 CIP-004-1 R1 - OVERVIEW

WECC determined that URE did not document and implement security and personnel risk assessment (PRA) programs under CIP-004-1. Specifically, URE failed to establish, maintain, and document a security awareness program as required by CIP-004-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing requirements, training and awareness programs, and current record retention capabilities to identify any such processes that possess applicability for the NERC CIP requirements;
2. design and implement a cyber security awareness program for all employees, vendors, and contractors for all qualifying CCAs pursuant to the requirements of CIP-004 R1;
3. create and maintain a document repository to identify, track, and audit employees, vendors, and contractors for cyber awareness completion; and
4. document and implement a procedure to ensure that the cyber awareness reinforcements are delivered on a quarterly basis.

WECC201002177 CIP-004-1 R2 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to establish, maintain, and document an annual cyber security training program, as required by CIP-004-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. implement a NERC CIP cyber security training program for all personnel with any access to CCAs;

2. implement the cyber security training program for all employees, vendors, and contractors for all qualifying Critical Assets and document attendance and completion of the training; and
3. document and implement a procedure to review and verify that the training was conducted on an annual basis.

WECC201002178 CIP-004-1 R3 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to have a documented PRA program and failed to conduct PRAs as required by CIP-004-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review and ensure that all individuals having authorized cyber or authorized unescorted physical access to CCAs possess an equivalent identify verification and seven-year criminal record check pursuant to CIP 004-R3.1;
2. identify and implement changes to contract clauses and conditions of employment as necessary to enable URE to complete elementary ID and criminal check risk assessments for on-boarding entity and contract staff (prior to staff being granted access);
3. establish and implement a procedure to prompt for personal re-reviews no less frequently than every seven years; and
4. document an annual process to review and ensure that the appropriate documentation for all assessments results is maintained pursuant to CIP-004, R3.3.

WECC201002179 CIP-004-1 R4 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs as required by CIP-004-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing URE policy and procedures to identify existing requirements, current practices, and the current status of all individuals who have been granted logical and physical access to systems that now include those that may be defined as CCAs;

2. establish requirements and delegated authority to grant logical and physical access to ESPs and Physical Security Perimeters (PSPs);
3. prepare lists of individuals who have been granted logical and physical access based on lists of CCAs, ESPs, PSPs; and
4. document a procedure to ensure that all documentation related to CIP-004 R4 is maintained pursuant to CIP-004.

WECC201002180 CIP-009-1 R1 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to create CCA recovery plans as required by CIP-009-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. expand or amend the current backup and recovery procedures;
2. promulgate the revised procedures and establish/identify organizational parties; and
3. establish and implement a reminder solution for a test of the backup recovery plan at least once each year.

WECC201002181 STANDARD REQ - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to exercise CCA recovery plans as required by CIP-009-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure local procedures are aligned with program guidance;
2. ensure local procedures are implemented and evidence collection has begun for Critical Asset facilities; and
3. evaluate and confirm cyber security recovery plan testing is implemented.

WECC201002182 CIP-009-1 R3 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices.

Specifically, URE failed to update CCA recovery plans to reflect changes or lessons learned as required by CIP-009-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to ensure that the recovery plans are updated to reflect any changes or lessons learned as a result of exercises or recovery from an actual incident.

WECC201002183 CIP-009-1 R4 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to have recovery plan(s) that included processes and procedures for the backup and storage of information required for the restoration of CCAs as required by CIP-009-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to ensure that the recovery plans include processes and procedures for the backup and storage of information required to successfully restore each CCA.

WECC201002184 CIP-009-1 R5 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to test backup media to ensure that information essential to system recovery is available as required by CIP-009-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to test information essential to recovery that is stored on backup media and establish a procedure to test annually thereafter that the information is available.

WECC201002186 CIP-005-1 R1 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to create and maintain a physical security plan as required by CIP-005-1 R1 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review all serial non-routable access into URE ESPs that rely on entity-owned communications systems and identify all valid access points;

2. review all serial non-routable access into URE ESPs that rely on public-switched telephone networks communications and validate that an ESP is defined for any dial-out or dial-up accessible CCAs that utilize non-routable protocols for that single access point at the dial-up device;
3. validate that the endpoints of communication links between discrete ESPs are included as access points with their respective ESPs and define the access points for each link; and
4. validate that all ESP network diagrams, inventories, and vulnerability assessments identify all interconnected systems, all access points into the ESP, and all Cyber Assets deployed for access control and monitoring of the access points.

WECC201002187 CIP-005-1 R2 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement physical access controls pursuant to CIP-005-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. develop a design for the access points associated with the serial non-routable communication links. The design will provide a Cyber Asset as the access point that is external to the CCA that supports the serial communications;
2. validate that all Cyber Assets utilized in the control and monitoring of the serial non-routable ESP access points are protected in accordance with the measures listed in CIP-005 R1.5. If the appropriate controls could not be provided, TFEs were processed;
3. implement the design and adjust the access control procedures to incorporate the changes; and
4. validate that an approved and documented process exists supporting access requests into the ESP.

WECC201002188 CIP-005-1 R3 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement technical and procedural controls for monitoring physical access to PSPs pursuant to CIP-005-1 R3 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. configure, validate, and document that an electronic monitoring capability is implemented for monitoring and logging non-routable access into the ESP and identified any approved TFE that is applicable to CIP-005 R3.2;
2. implement and document the electronic monitoring capabilities for dial-up accessible CCAs that utilized non-routable protocols; and
3. establish and validate the documented procedure that ensures the timely and periodic review and analysis of electronic access alarms for failed communication attempts to the ESP.

WECC201002189 CIP-005-1 R4 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to record sufficient information to identify individuals and access to PSPs uniquely pursuant to CIP-005-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify the type, scope, and test results for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in developing test procedures, addressing any identified vulnerabilities, or testing for minimal ports and services;
2. develop and promulgate the CIP vulnerability assessment procedures. The assessment was completed and documented;
3. employ test procedures and document the results of the test procedures for each identified ESP access point;
4. prepare a mitigation plan addressing the correction of vulnerabilities identified;
5. ensure that the vulnerability assessment verifies ports and services permitted through the access control device, as well as ports and services open for management of the device; and
6. ensure the vulnerability assessment includes the discovery of all ESP access points, including verification that each serial access point is configured as documented in the network diagram.

WECC201002190 CIP-005-1 R5 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to retain physical access logs as required under CIP-005-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and place the appropriate documentation artifacts from the following document types under management control: guidance documents, process documents, configuration documents, and event documents;
2. validate documentation process to ensure that management control of documentation meets CIP-005 requirements;
3. review asset inventory spreadsheets for accuracy and validate inventory assets associated with each Critical Asset;
4. review all CIP-005-related documents, including procedures and configuration documents and verify their accuracy; and
5. ensure timely update of change management procedures as required by CIP-005.

WECC201002198 CIP-003-1 R1 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy pursuant to CIP-003-1. Instead, for the management of protection for CCAs, URE relied on a federal cyber security policy. Specifically, URE failed to document or implement a cyber security policy as required by CIP-003-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. design the approach, structure, and organization for integrating and documenting the NERC CIP cyber security standards as URE policy;
2. determine structure and organization of cyber security policy for NERC CIP compliance pursuant to existing organizational governance;
3. develop general cyber security policy document that will provide authorization for URE to implement the NERC CIP Standards;

4. develop directives, standards, and associated guidance documents that provide URE staff direction to identify Critical Assets and CCAs and achieve compliance; and
5. identify an activity tracking item to provide an annual prompt no less than 30 days in advance of the annual review date for the policy.

WECC201002199 CIP-003-1 R3 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy pursuant to CIP-003-1. Instead, for the management of protection for CCAs, URE relied on a federal cyber security policy. Specifically, URE failed to document exceptions in instances in which it could not conform to its cyber security policy, as required by CIP-003-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify exceptions from the promulgated policy that are necessary for installed and planned cyber systems that qualify under the NERC CIP requirements;
2. review submitted exception request rationale for reasonability and risk and forward qualifying exception requests to the senior manager responsible for final review and signature;
3. secure the approval of the NERC CIP policy exceptions from the senior manager responsible for the NERC CIP effort; and
4. formally document the reviews and approvals.

WECC201002200 CIP-006-1 R1 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a federal cyber security policy. Specifically, URE failed to create and maintain a physical security program as required by CIP-006-1 R1 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. develop the security plan template and promulgate it to all system owners for an initial assessment regarding the scope of impact to existing physical security systems and security operations;
2. perform initial reviews and comments. Revisions to the template or process updates were considered accordingly;

3. submit final physical security plans;
4. establish and implement a reminder solution for an annual review;
5. implement the physical security plans per NERC CIP Requirements CIP-006 R2 through R8; and
6. review physical security plans.

WECC201002201 CIP-006-1 R2 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a federal cyber security policy. Specifically, URE failed to document and implement physical access controls pursuant to CIP-006-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and inventory all existing or planned physical security systems that authorize and/or log access to ESPs and CCAs;
2. conduct initial assessments and cost estimations to align the existing physical security systems identified;
3. ensure that all final PSPs submitted as final pursuant to CIP-006 R1, included and addressed compliance with the standards;
4. execute any associated design, procurement, or installation plans; and
5. complete all tasks and activities associated with plans identified.

WECC201002202 CIP-006-1 R3 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement technical and procedural controls for monitoring physical access to PSPs pursuant to CIP-006-1 R3 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review to ensure that all prerequisites have been completed;
2. verify that all Cyber Assets used in the access control and/or monitoring of the ESPs reside within a PSP;

3. ensure that Cyber Assets that exist within a PSP are documented in the physical security plan; and
4. develop and execute plans to move or encapsulate the Cyber Assets within a PSP, for Cyber Assets that do not exist in a PSP.

WECC201002203 CIP-006-1 R4 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to record sufficient information to identify individuals and access to PSPs uniquely pursuant to CIP-006-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the physical access control requirements in CIP-006 R4 and identify the type of physical access methods implemented at all access points;
2. ensure that the PSPs address and include operational and procedural controls to manage physical access 24 hours a day, seven days a week; and
3. implement all physical access control capabilities and methods identified in the physical security plan.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed no penalty for the referenced violations. In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-certified the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations posed a moderate and not a serious or substantial risk to the reliability of the BPS; and

6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC has assessed no penalty for the referenced violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Gizelle Wray* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile gizelle.wray@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement
Gizelle Wray*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

April 27, 2017

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

URE have entered into Settlement Agreements[4] to resolve all outstanding issues arising from WECC's determination and findings of violations of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreements, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred and one thousand dollars ($201,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreements.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreements, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreements and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreements by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreements.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC2015014909	CIP-006-3c	R2.2	Medium/ High	SR	Moderate	$201,000
WECC2015015031	CIP-004-1	R3	Lower/ Moderate			

WECC2015014909 CIP-006-3c R2.2- OVERVIEW

WECC determined that URE did not afford the protective measures of CIP-007-3a R5.1.1 to its Physical Access Control System (PACS). Specifically, URE reported that during a review of its PACS

[4] NERC combined these settlement agreements into one Full Notice of Penalty for ease of review and efficiency. For CIP-004-1 R3, the final penalty was $113,000 and for CIP-006-3c R2, the final penalty was $88,000 for a total penalty of $201,000.

access list, URE discovered that one of its PACS administrators had received administrative rights to the PACS before the access was approved.[5] During communications with WECC, URE determined that it had a second instance of possible noncompliance because it had one virtual server that was not previously identified as an in-scope asset as part of its PACS. The one virtual server monitored and controlled access for the Physical Security Perimeters (PSPs) at 29 different Critical Assets.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). In the first instance, URE failed to ensure that administrative rights to a PACS were approved prior to being granted. The risk was partially reduced by the fact that the individual who received access prior to the requisite approval had a valid personnel risk assessment (PRA) and successfully received approved access within seven days. In the second instance, URE failed to include one virtual server within its PACS as required by CIP-006-3c, and therefore did not afford it all of the required protective measures. Nevertheless, if an unauthorized attempt to access the virtual server had occurred, URE had controls in place that would have generated an alert, and URE's incident response procedures would have started an investigation.

WECC determined the duration of the violation to be approximately 1,580 days, from the date when one employee was granted administrative rights to a PACS prior to obtaining proper approvals, through when URE completed its NERC CIP PACS security system upgrade, to include eight new hypervisors, and applied all applicable protective controls to the upgraded security system.

To mitigate this violation, URE:

1. finalized access approvals for one employee;
2. provided all applicable URE employees with cyber security training to reinforce the requirement to obtain proper approval prior to provisioning access to any Cyber Asset;
3. completed its NERC CIP PACS security system upgrade, to include eight new hypervisors, and applied all applicable protective controls to the upgraded security system; and
4. updated its procedures to include a process to regularly monitor and ask for compliance guidance from WECC for Reliability Standard interpretations.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

[5] URE personnel approved the access seven days after the improper granting of administrative rights.

WECC2015015031 CIP-004-1 R3 - OVERVIEW

WECC determined that during an assessment of URE's PRA records, URE discovered a discrepancy between the social security number (SSN) and date of birth (DOB) listed for an individual with physical access to a URE PSP. Specifically, URE had conducted the initial PRA using an incorrect SSN and DOB. Because of this discrepancy, URE initiated a review of the records of all individuals with authorized electronic or unescorted physical access to Critical Cyber Assets (CCAs) since the enforceable date of CIP-004-1 R3. This review revealed 74 erroneous PRAs, 12 individuals who were granted CIP access without a validated PRA, and five individuals who had expired PRAs without CIP access being revoked.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's inadequate PRA procedures failed to ensure 91 individuals with authorized electronic or unescorted physical access to CCAs had completed a PRA as required by CIP-004-1—creating a potential vulnerability. The violation's risk was reduced because the individuals were otherwise authorized to have logical and/or unescorted physical access to CCAs. Moreover, the authorized individuals completed annual CIP training and were in good standing with URE.

WECC determined the duration of the violation to be approximately 2,193 days, from the date the Reliability Standard became mandatory and enforceable, through when URE completed the last renewal of the PRAs.

To mitigate this violation, URE revised its PRA and procedure document to address any employee contact information discrepancies or alias issues.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreements, WECC has assessed a penalty of two hundred and one thousand dollars ($201,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered the instant violations as repeat noncompliance with the subject NERC Reliability Standards and determined the compliance history should serve as an aggravating factor;
2. URE had an internal compliance program (ICP) at the time of the violation. Nevertheless, WECC did not give credit for URE's ICP because WECC determined that if the ICP had been

implemented properly, URE would have been able to identify, assess, and correct these violations in a timely manner;

3. URE self-reported the violations; however, WECC did not apply self-reporting credit to the penalty amount because of the duration between URE's discovery and self-reporting of the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of WECC2015014909 and WECC2015015031 posed a moderate and not a serious or substantial risk to the reliability of the BPS;
7. WECC considered the duration of the violations as an aggravating factor; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred and one thousand dollars ($201,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreements and supporting documentation on March 23, 2017 and approved the Settlement Agreements. In approving the Settlement Agreements, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreements and believes that the assessed penalty of two hundred and one thousand dollars ($201,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel, Corporate Secretary Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Gizelle Wray* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile gizelle.wray@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Gizelle Wray
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 31, 2017

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP17-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

NERC respectfully requests that the Commission accept this Spreadsheet NOP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction, or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Request for Confidential Treatment

NERC is submitting this information on July 31, 2017 and requests the information contained within Attachment A-3 be treated as Confidential and Critical Energy/Electric Infrastructure Information (CEII). NERC requests this designation apply to the included information for five years.[7] A public version of this attachment is included as Attachment A-2. The requested duration is appropriate as the information includes Confidential CEII information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as other Confidential information as defined in the NERC ROP including the NERC CMEP Appendix 4C to the ROP. Protecting this information is necessary to ensure the safety and security of the bulk power system. This filing includes non-public information related to certain Reliability Standard noncompliance and other confidential information inextricably intertwined with CEII.[8]

In accordance with the Commission's Regulations, 18 C.F.R. §§ 388.113, NERC is providing a redacted public version of the information separately.

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

[7] *See FAST Act*, Pub. L. No. 114-94, § 61,003, 129 Stat. 1312, 1773-1779 (2015); *see also* 18 C.F.R. § 388.113(d)(1)(i-ii).

[8] 18 C.F.R. § 388.113(g)(5)(ix).

Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	Region	Registered EntityName	NCR	NERC Violation ID	Notice of Confirmed Violation or Settlement Agreement
2	ReliabilityFirst Corporation (ReliabilityFirst or RF)	Unidentified Registered Entity 1 (ReliabilityFirst_URE1)	NCRXXXXX	RFC2014013842	Settlement Agreement

	F
1	Description of the Violation
2	ReliabilityFirst_URE1 submitted a Self-Report stating that it had an issue with CIP-007-3a R3.1. Additionally, the Regions determined that ReliabilityFirst_URE1 had an issue of CIP-007-3a R3 as a result of a Compliance Audit. The violation at issue concerns ReliabilityFirst_URE1's execution and documentation of security patch assessments by a subset of ReliabilityFirst_URE1's Information Technology (IT) group. The subset of the IT group maintains a separate NERC CIP SCADA environment, which was the subject of the violation. The servers in this domain support the applications, including the the Energy Management System (EMS), used by the ReliabilityFirst_URE1 Dispatch groups to perform real-time dispatch functions for ReliabilityFirst_URE1's power plants. The total number of unique devices impacted was 3% of ReliabilityFirst_URE1's CIP devices (during the time period of the violation). During Self-Certification activities and the Compliance Audit, ReliabilityFirst_URE1 and the Regions identified three sets of missed patch assessments. First, as part of Self-Certification activities, ReliabilityFirst_URE1 discovered that it did not assess patches released on certain devices. ReliabilityFirst_URE1 determined that assessments for those months were overlooked at the time the patches were released and thus not timely assessed or implemented. After discovering the issue, ReliabilityFirst_URE1 assessed the security patches released and determined that 11 security patches were applicable to ReliabilityFirst_URE1's Cyber Assets. These 11 patches affected 88 devices that support SCADA and EMS functions in ReliabilityFirst_URE1's dispatch unit, which is responsible for dispatching power plants across ReliabilityFirst_URE1's entire footprint. Second, during the Compliance Audit, the Regions identified additional instances of ReliabilityFirst_URE1's IT group not timely documenting the assessment of patches and security upgrades on devices that support the dispatch systems. During the audit, the Regions requested evidence of assessments for security patches released by certain third-party vendors that were potentially applicable to devices that support dispatch systems. ReliabilityFirst_URE1 was unable to provide sufficient evidence that it assessed these patches in a timely manner. Instead, in some cases, ReliabilityFirst_URE1's documented assessments were incomplete, and in other cases, ReliabilityFirst_URE1 did not have sufficient documentation relating to its monthly checks for released patches and thus was unable to provide evidence to show whether or not patches were released by the vendors. After the audit, ReliabilityFirst_URE1 conducted a review of the patches released during those months to determine if ReliabilityFirst_URE1 missed patches that were applicable to its systems. As a result of that review, ReliabilityFirst_URE1 determined that the patches released by these third-party vendors during those months were not applicable to ReliabilityFirst_URE1 devices. The vendors at issue supplied software that ReliabilityFirst_URE1 ran on 64 devices. Third, during the Compliance Audit, ReliabilityFirst_URE1 provided evidence of an extent of condition review it conducted in response to the audit data request where it discovered 26 instances of late patches and missing or insufficient assessments for ReliabilityFirst_URE1's dispatch devices. The root cause of the violation was poor asset and configuration management controls, meaning that improved monitoring and oversight of the patch management process could have reduced the likelihood of occurrence. Oversight of this particular aspect of the process was inadequate, and there were inadequate documented patch management processes in place. Thus, as part of its mitigation, ReliabilityFirst_URE1 assigned an IT manager responsible for ensuring the successful completion of ReliabilityFirst_URE1's patch management program and created a formal documented process for patch management for these groups at

	G	H	I	J	K
1	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
2	CIP-007-3a	R3; R3.1	Lower	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The delay in or failure to assess, document, and implement security patches, especially relating to patches for ReliabilityFirst_URE1's EMS, could potentially allow a vulnerability to be exploited, which could affect the neighboring entities visibility into the system. Additionally, the violation occurred over a long duration and affected 93 devices that serve critical functions across ReliabilityFirst_URE1's entire footprint. And, because the Regions determined the root cause was a lack of management controls surrounding the patch management processes, the violation was widespread within the generation dispatch unit and there was a risk that the violation could have continued, thus potentially affecting the systems for a longer period. However, because of the facts and circumstances particular to this violation, including the multiple significant protections in place at the time of the violation, the Regions determined that the violation posed moderate risk to the reliability of the BPS. More specifically, the risks were partially mitigated by the following factors. First, ReliabilityFirst_URE1's security approach incorporates the traditional practices of layered firewalls, intrusion detection/prevention systems, security event monitoring and antivirus, but, importantly, also includes more sophisticated systems and protections going beyond traditional defense-in-depth techniques. Some of these significant protections include ReliabilityFirst_URE1's approach to host-based protections, network protections, and monitoring and proactive threat mitigation. ReliabilityFirst_URE1's monitoring includes end-point data and intelligence monitoring–including inbound and outbound anomalous network traffic. Across ReliabilityFirst_URE1's footprint, it operates a single network with very limited Internet connections. ReliabilityFirst_URE1 uses multiple industry leading advance persistent threat tools for both monitoring and auto-blocking cyber threats, ranging from common malware to near zero-day type attacks. Importantly, ReliabilityFirst_URE1 was able to demonstrate that, because of its approach, its system was protected against the specific vulnerabilities for which patches were released for the subject Cyber Assets throughout the duration of the violation. These combined protection and detection methods make it less likely that any vulnerability remediated by an identified patch would have been exploited. The Regions also note that the violation affected only one business unit, generation dispatch, and thus potential impact of a compromise would be limited to the function of that business unit. (ReliabilityFirst_URE1 indicated that with respect to the potential impact, in the event of compromise, the neighboring entities would redeploy any regulation service to other non-ReliabilityFirst_URE1 generators, and ReliabilityFirst_URE1 dispatchers would call the neighboring entities to ensure ReliabilityFirst_URE1 units were doing what the neighboring entities operators were requesting. These calls would occur periodically allowing the neighboring entities to

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	L	M	N	O	P
1	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity
2	the first date ReliabilityFirst_URE1 was late in documenting the assessment of a security patch	when ReliabilityFirst_URE1 performed the final outstanding patch assessment	$150,000	Self-Report	To mitigate this violation, ReliabilityFirst_URE1: 1) conducted an investigation into patches for the months in question and a review of the sources for potential patches during that time indicated that none of the patches released were applicable to ReliabilityFirst_URE1's CIP environment; 2) assessed and implemented the latest versions of the patches at issue regarding the additional 26 instances identified during the Compliance Audit; 3) completed the missed security patch assessments; 4) assigned an IT Manager responsible for ensuring the successful completion of the IT security patch management program. This includes a documented process for conducting assessments and documenting assessment results; 5) developed a project plan to identify resources and tasks needed to implement process improvements, including increased automation through the use of an electronic tool; 6) reviewed all of the IT security patch management processes and controls to determine the current state of the processes, including compliance gaps. This included an extent of condition review; 7) implemented an electronic tool to monitor and track security patch assessments, including automated notification processes, new dashboards, and reports; and 8) included a process, within the electronic tool described above, for creating or revising mitigation plans when applicable patches are unable to be applied within 35 days of evaluation completion.

	Q	R	S	T
1	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
2	12/12/2015	11/9/2016	Neither Admits nor Denies	The Regions considered certain aspects of ReliabilityFirst_URE1's internal compliance program and awarded mitigating credit. Additionally, in response to the current violation, ReliabilityFirst_URE1 voluntarily implemented a mitigation strategy with strong overarching milestones, which is indicative of a strong compliance program. However, the Regions determined that full credit was not warranted because the current violation was indicative of a weakness in the patch management aspect of ReliabilityFirst_URE1's compliance program. The Regions considered ReliabilityFirst_URE1's cooperation during the Settlement Agreement process and awarded mitigating credit. Although ReliabilityFirst_URE1 struggled to provide the Regions with an accurate full scope of the violation and complete evidence of Mitigation Plan completion, ReliabilityFirst_URE1 attempted to cooperate with ReliabilityFirst throughout the enforcement process. The difficulty in providing the Regions with accurate and useful evidence of mitigation plan completion made it difficult to verify that ReliabilityFirst_URE1 satisfactorily completed its mitigation plan. ReliabilityFirst_URE1 and the Regions have discussed this issue, and ReliabilityFirst_URE1 is aware that it must apply a higher standard in the future when certifying mitigation plans so that verification is not delayed. Since ReliabilityFirst_URE1 acted in good faith and intended to be cooperative throughout the duration of the Compliance Audit and enforcement action, the Regions applied some mitigating credit for ReliabilityFirst_URE1's cooperation. As above and beyond actions, ReliabilityFirst_URE1 has spent more than $1.7 million implementing a baseline monitoring software that scans selected assets nightly (including those associated with this violation) and reports any changes discovered. The tool will report any security patches that get applied in this nightly assessment. The tool also collects application versions and updates daily. Anything that the tool identifies as outside of the current baseline for a device is flagged as an exception and investigated by

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	Region	Registered EntityName	NCR	NERC Violation ID	Notice of Confirmed Violation or Settlement Agreement
3	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity (WECC_URE_2)	NCRXXXXX	WECC2016016130	Settlement Agreement

	F
1	Description of the Violation
	WECC_URE_2 submitted a Self-Report stating that it had a possible issue of noncompliance with CIP-006-3c R2.1 and R2.2. For the first instance, during an upgrade to WECC_URE_2's Physical Access Control Systems (PACS), WECC_URE_2 failed to provide all the protections of CIP-006-3c R2.2 to 14 PACS workstations that were commissioned with software. WECC_URE_2 discovered this instance while performing an internal audit in preparation for the upcoming WECC audit. WECC_URE_2 hired a third-party company to further investigate the results of its internal audit. The results of the investigation determined that 1) WECC_URE_2 was noncompliant with CIP-006-3c R2.1 for not protecting all 14 workstations from unauthorized physical access, and 2) WECC_URE_2 failed to afford the protections, as described below, pursuant to CIP-006-3c R2.2, relating to the 14 workstations: a. CIP-003 R4: Not included in the information protection plan; b. CIP-003 R6: NERC change control procedures were not in place; c. CIP-004 R3: Initial and renewed Personnel Risk Assessments every 7 years were not validated for personnel with unescorted physical access; d. CIP-005 R2: The firewalls did not document and restrict ports/services with the same rigor as required in NERC CIP. Remote access to these workstations was allowed from corporate devices, and there is no CIP-compliant two-factor authentication for remote access; e. CIP-005 R3: Corporate networks and the corporate firewalls were monitoring for alerting for detected threats, but not with the scrutiny as required in this Standard; f. CIP-006 R4: Physical access controls were insufficient; g. CIP-006 R6: No logging records for three of the PACS workstations; h. CIP-007 R1: No testing conducted prior to commissioning; i. CIP-007-R2: Did not ensure only required ports and services were enabled; j. CIP-007 R3: Did not ensure patches were tracked, evaluated, tested, and installed; k. CIP-007 R4: Did not ensure anti-virus signature updates were tested prior to being installed; l. CIP-007 R5: Did not annually review user access rights; m. CIP-007 R7: Not included in appropriate disposal and redeployment policy; and n. CIP-007 R8: Did not perform annual cyber vulnerability assessments. The root cause of the first instance was an internal misunderstanding of the applicability of CIP-006-3c R2.1 and R2.2 to PACS workstations. For the second instance, WECC_URE_2 failed to provide all the protective measures of CIP-006-3c R2.2 when it did not change the password for one shared account on five PACS Internal Controller (IC) boards, annually. The shared account resided on all five IC boards.
3	

	G	H	I	J	K
1	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment
3	CIP-006-3c	R2; R2.1; R2.2	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In the first instance, WECC_URE_2 failed to provide the protective measures of CIP-006-3c R2.1 and R2.2 to 14 PACS workstations. In the second instance, WECC_URE_2 failed to provide the protective measures of CIP-006-3c R2.2 to five PACS IC boards. Failure to adequately protect cyber assets that provide, monitor, and log physical access to the Critical Cyber Assets (CCAs) integral to the reliable operation of the Bulk Electric System (BES) could compromise the CCAs or allow an unauthorized individual with malicious intent to have access to the CCAs; thus, potentially affecting the reliability of the Bulk Power System (BPS). The likelihood of these risks occurring were reduced by the controls implemented by WECC_URE_2. Specifically, WECC_URE_2 had 24 hour-a-day, 7 day-a-week access monitoring and security event monitoring on the CCAs with the PSPs. WECC_URE_2 had policies and procedures restricting access to only authorized personnel, as well as regular reviews of the personnel with electronic and/or unescorted physical access and their specific access privileges. WECC_URE_2's corporate firewalls were restricted based on corporate policies. A "deny all" firewall rule was present. Ports and services to and through the access points were restricted. WECC_URE_2 had an active Intrusion Prevention System (IPS) monitoring and preventing any unknown or suspicious inbound traffic into the network. Corporate firewalls were monitored by a product which detects any changes made to the firewalls for investigation into whether the change was authorized. Physical access to any workstation required a valid WECC_URE_2 badge. All but four of the 14 workstations were within restricted rooms, where access to the building or room required individual badging. The four workstations not in restricted buildings or rooms still required a WECC_URE_2 badge and were monitored by employees during working hours. Changes to the workstations were limited to administrators only. WECC_URE_2 restricted ports on its corporate firewalls and had implemented a network-based IPS that could detect unexpected ports and services. The IC boards are naturally restrictive devices with limited functionality and no direct human interface capability. This reduced the potential that an unauthorized individual would be able to gain logical access to the IC boards. The IC boards are all within designated PSPs where access is restricted, logged, and monitored. Additionally, all personnel who were granted logical access to the PACS workstations and IC boards had training and current Personnel Risk Assessments. No harm is known to have occurred.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	L	M	N	O	P
1	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity
3	The first instance began when WECC_URE_2 did not provide protective measures to 14 PACS workstations	The first instance ended upon mitigation completion The second instance ended when WECC_URE_2 changed the password on one shared account.	$74,000	Self-Report	To mitigate this violation, WECC_URE_2: 1) Assessed whether all 14 workstations are needed; 2) Designated the remaining workstations as PACS devices; 3) Identified the most secure location for workstations assessed as being needed; 4) Designed a plan to ensure the remaining workstations have the physical and logical protections required by CIP Version 6; 5) Implemented the workstation CIP Version 6 plan; 6) Changed the passwords on the IC boards; 7) Identified and documented firmware versions on the IC boards; 8) Performed a comprehensive review of the IC boards to ensure compliance with applicable Standards; and 9) Documented ownership of the IC boards.

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	Q	R	S	T
1	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
	6/26/2017	TBD	Admits	WECC reviewed WECC_URE2's internal compliance program (ICP) and considered it a neutral factor in the penalty determination. Although WECC_URE_2 has a documented ICP that has been provided to WECC, WECC determined that because WECC_URE_2 did not implement their ICP with effective internal controls to identify this issue timely, the ICP does not qualify for credit. WECC_URE_2 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit/during the self-certification period. WECC considered WECC_URE_2's CIP-006 R2 compliance history in determining the penalty. WECC_URE_2's relevant prior noncompliance with CIP-006 R2 includes two prior violations. WECC considered WECC_URE_2's CIP-006 R2 compliance history to be an aggravating factor in the penalty determination.
3				

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 2017

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of violations of NERC Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2017). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE admits to the violations, and has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SPP RE and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement and herein.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SPP2014014499	CIP-003-3	R2: R2.2	Medium/ Severe	CA	Minimal	$250,000
SPP2014014500	CIP-003-3	R6	Lower/ Severe		Moderate	
SPP2014014513	CIP-004-3a	R4	Lower/ Moderate			
SPP2014014514	CIP-005-3a	R1: R1.5; R1.6	Medium/ Severe			
SPP2014014501	CIP-006-3c	R1: R1.6.1	Medium/ Severe			
SPP2014014502	CIP-006-3c	R2: R2.2	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SPP2014014505	CIP-007-3a	R1: R1.1	Lower/ Severe	CA	Moderate	$250,000
SPP2014014506	CIP-007-3a	R2: R2.1; R2.2	Medium/ Severe			
SPP2014014507	CIP-007-3a	R4: R4.1	Medium/ Severe			
SPP2014014508	CIP-007-3a	R5: R5.2; R5.2.2	Lower/ Severe			
SPP2015015324	CIP-007-3a	R6: R6.1; R6.4; R6.5	Medium/ Severe			
SPP2014014510	CIP-008-3	R1: R1.6	Lower/ High			
SPP2014014511	CIP-009-3	R2	Lower/ Severe			

SPP2014014499 CIP-003-3 R2: R2.2 - OVERVIEW

SPP RE determined that URE, on multiple occasions, did not document, within 30 calendar days of the effective date, changes to the senior manager assignment with overall responsibility and authority for leading and managing its implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

SPP RE determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). URE attested that a CIP senior manager was in place and responsible for implementation of the URE CIP Compliance program and that there were no cyber security incidents during the time of the violation.

SPP RE determined the duration of the violation to be approximately 10 months, from the date URE failed to document the change in assigned senior manager, through when URE completed its leadership delegation document identifying the senior manager.

To mitigate this violation, URE:

1. reviewed the URE cyber security policy and identified improvements to ensure compliance with CIP-003 R2;
2. updated the cyber security policy based upon recommendations from the policy review;
3. documented the assignment of the current CIP senior manager; and
4. developed a new URE leadership document to include responsibilities for implementing the process and designation of the CIP senior manager and delegates.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014500 CIP-003-3 R6 - OVERVIEW

SPP RE determined that URE did not: 1) design documentation controls supportive of the designed change management process; and 2) execute the change management process as documented. Specifically, there were deficiencies in URE's change request form when compared with the documented change management process. Additionally, URE's change request form for several changes were missing information and thus did not adhere to the URE change management process.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE had a change control process in place at the time of the violation. The affected assets were behind a firewall. URE's Critical Cyber Assets (CCAs) require an authorized user name and password combination to gain access. URE personnel with access to CCAs had CIP training and current personnel risk assessments (PRAs). The CCAs subject to this violation resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 40 months, from the completion date of the mitigation for the prior violation of the same standard and requirement, through the date URE implemented its updated CCM program that controls changes to CCAs.

To mitigate this violation, URE:

1. redesigned its change management process;
2. implemented system monitoring software to support its change management process;

3. implemented change management software to support controls for its change management process; and
4. updated change management process documentation.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014513 CIP-004-3a R4 - OVERVIEW

SPP RE determined that URE did not maintain an accurate list of personnel with authorized unescorted physical access to CCAs. URE authorized its Physical Access Control Systems (PACS) vendor to grant some vendors and a URE employee access to URE's Physical Security Perimeters (PSPs). The PACS vendor mistakenly granted access for over 90 URE employees who were authorized for access to specific, but not all, PSPs.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Most of the employees mistakenly granted access to all PSPs did not know they were granted access. There was one unauthorized access to a PSP, which was reported by the offender. URE's CCAs are physically and electronically segregated. The assets subject to this violation reside within a physical access-controlled data center; the area with CCAs is staffed 24/7, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately one month, from the date the vendor mistakenly granted access to its PSPs for over 90 URE employees, through the date URE removed the unauthorized PSP access for all personnel that had mistakenly been granted such access.

To mitigate this violation, URE:

1. revoked access to the PSPs for the employees who were not authorized to have such access;
2. reviewed and revised the asset list for accuracy; and
3. developed an internal procedure to prevent the creation of accounts prior to granting approved access.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014514 CIP-005-3a R1: R1.5; R1.6 - OVERVIEW

SPP RE determined that URE did not maintain documentation of its Electronic Security Perimeters (ESPs). Specifically, URE failed to: 1) identify and document all access points to the ESPs in violation of R1; 2) ensure that Cyber Assets used in the access control and/or monitoring of the ESPs were afforded protective measures as specified in CIP-003-3 R6 in violation of R1.5; and 3) maintain documentation of its ESP(s), all electronic access points to the ESP(s), and the Cyber Assets deployed for the access control and/or monitoring of access points (EACMs) in violation of R1.6. In the first instance, the servers essential to performing strong authentication for remote interactive access to URE's ESPs were not properly identified as EACMS, in violation of R1. In the second instance, URE did not properly perform its documented change management process when applying changes to its EACMS devices, in violation of R1.5. In the third instance, URE had deficient ESP documentation, in violation of R1.6.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. URE's Cyber Assets resided within a physical access-controlled data center and behind a firewall. Access to Cyber Assets within the PSP was limited to only those with authorized physical and/or electronic access rights. The area with CCAs used in real-time operations of the BPS was staffed 24/7. URE had 24-hour closed-circuit television monitoring of the PSP locations, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 32 months, from the date the first change in assets was not reflected in the ESP diagram, through the date URE reviewed the CCA List and ESP diagram and updated the ESP diagram.

To mitigate this violation, URE:

1. disabled remote access to the EACMS Cyber Assets;
2. updated the change management process to include a step for reviewing and reconciling the CCA list and ESP documentation; and
3. reviewed the CCA list and ESP diagram and updated the ESP diagram to resolve any discrepancies.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014501 CIP-006-3c R1: R1.6.1- OVERVIEW

SPP RE determined that URE did not properly document the entry and exit of visitors, including the date and time, to and from its PSP. The Audit Team discovered over 20 instances where visitors' entry and/or exit times were not recorded.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE implemented password complexity and lockout policies to reduce the risk of unauthorized access. All personnel with authorized access to Cyber Assets had CIP training and current PRAs. URE's Cyber Assets resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. A majority of the deficient log entries were for janitorial staff who had completed cyber security training and possessed a valid PRA.

SPP RE determined the duration of the violation to be over 27 months, from the day after completion of the mitigation plan for a previous violation of the same Standard and requirement, through the last recorded instance of a deficient visitor log entry.

To mitigate this violation, URE:

1. began maintaining separate visitor logs for each of the PSPs and the common area of the building;
2. updated the visitor access procedure;
3. trained applicable URE personnel on the new visitor access procedure;
4. added a process for review and validation of visitor logs on a daily and quarterly basis to confirm that visitor log procedures have been followed and to promptly address any issues. Identified issues will be documented and reported via a new policy exception form; and
5. instituted periodic compliance spot checks to validate the proper execution of the visitor access policies and procedures.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014502 CIP-006-3c R2: R2.2- OVERVIEW

SPP RE determined that URE did not provide its PACS the protective measures specified in CIP-003-3 R6, CIP-007-3 R2.1, and CIP-007-3 R2.2 when a change was made to the PACS without appropriate

change control or security controls testing. Cyber Assets that authorize and/or log access to PSP(s), exclusive of hardware at the PSP access point(s), were not afforded the protective measures in CIP-003-3 R6. Specifically, URE failed to implement its change management process when making changes to the PACS workstation server, and change request forms for several changes involving PACS were incomplete and thus did not adhere to URE's change management processes. URE failed to implement its process to ensure only those ports required for normal and emergency operations were enabled as required by CIP-007-3 R2.1 and that all other ports were disabled as required by CIP-007-3 R2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. The PACS resided on a network separate from URE's energy management system, with a firewall separating it from the corporate network. The PACS host server resided within a PSP, requiring local access to manage, add users, or make system changes. All personnel with access to Cyber Assets had CIP training and current PRAs. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 30 months, from the day after completion of the mitigation plan for a previous violation of the same Standard and requirement, through the date URE implemented its updated change management program.

To mitigate this violation, URE:

1. redesigned its change management process;
2. implemented system monitoring software to support its change management process;
3. implemented change management software to include controls for its change management process; and
4. updated change management process documentation.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014505 CIP-007-3a R1: R1.1 - OVERVIEW

SPP RE determined that URE did not implement cyber security test procedures in a manner that minimized adverse effects on the production system or its operation. URE implemented a system version update was implemented without prior installment in a testing environment, as required by URE's cyber security test procedures. Additionally, URE failed to demonstrate that testing had been

performed for a firewall configuration change, a switch configuration change, and a change involving operating system patching, as required by URE's change management procedure.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. The Cyber Assets subject to this violation resided within a physical access-controlled data center and behind a firewall. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be over 32 months, from the completion date of the mitigation plan for a prior violation of the same Standard and requirement, through when URE completed its mitigation.

To mitigate this violation, URE:

1. redesigned, implemented, and documented its change management program to include cyber security controls testing of all significant changes, including vendor changes; and
2. implemented system reports and alerts as detective and preventive controls to support change management.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014506 CIP-007-3a R2: R2.1; R2.2 - OVERVIEW

SPP RE determined that URE did not ensure that only ports and services required for normal and emergency operations were enabled on all Cyber Assets within the ESP. Specifically, URE failed to demonstrate the need for a number of ports and services open on its servers by either documenting them as being necessary, closing them, or obtaining a Technical Feasibility Exception (TFE). URE could not demonstrate that it had enabled only those ports required for normal and emergency operations as required by R2.1. As the enabled ports identified in R2.1 were not included in URE's documented ports baseline, URE was unable to ensure that other ports had been disabled prior to production use of the servers inside the ESP or were covered by a TFE as required by R2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place

at the time of the violation. The Cyber Assets subject to this violation resided within a physical access-controlled data center and behind a firewall. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 17 months, from the date of the cyber vulnerability assessment report that identified the undocumented ports, through the date URE documented and began controlling ports and services required for normal and emergency operations.

To mitigate this violation, URE:

1. requested a TFE for two PACS devices for which it is not technically feasible to configure ports and services;
2. reviewed the baselines to confirm which ports were required;
3. implemented a change management procedure to support review and update of baseline documentation; and
4. implemented software to monitor the ports and notify staff of any system changes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014507 CIP-007-3a R4: R4.1 - OVERVIEW

SPP RE determined that URE did not configure the anti-virus client properly during the installation of anti-virus and malware prevention software on an energy management system console. As a result, the software was unable to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on the console.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Only one console was involved in the violation. There were also protective measures in place at the time of the violation. The console resided within a physical access-controlled data center and behind a firewall. Where technically feasible, anti-virus and malware prevention tools were implemented on the other Cyber Assets located within URE's ESP. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. URE's Cyber Assets resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was

staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 24 months, from the date the console was commissioned without the implementation of anti-virus and malware prevention tools, through the date URE implemented the necessary software.

To mitigate this violation, URE:

1. configured the anti-virus software on the console;
2. updated the daily checklist to include more detailed information related to the status of anti-virus software running on Cyber Assets;
3. implemented software to report on anti-virus signature updates for all in-scope Cyber Assets;
4. configured anti-virus software to send email alerts and daily scan reports; and
5. configured system monitoring software to monitor the status of anti-virus running on all in-scope Cyber Assets capable of running anti-virus.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014508 CIP-007-3a R5: R5.2; R5.2.2 - OVERVIEW

SPP RE determined that URE did not document multiple shared default administrator accounts in URE's master account management list in accordance with URE's account management process per CIP-007-3 R5.2. Additionally, because the multiple shared default administrator accounts had not been documented on URE's master account management list, the individuals with access to such accounts were also not identified on the list per R5.2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE's CCAs require an authorized user name and password combination in order to gain access. All personnel with authorized access to Cyber Assets have CIP training and current PRAs. The Cyber Assets subject to this violation reside within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS is staffed 24/7, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately five months, from the date shared default administrator accounts and users of such accounts were incorrectly documented, through the date URE updated its checklist to reflect the correct system accounts and users.

To mitigate this violation, URE:

1. corrected the account list to reflect the actual default administrator account names;
2. implemented change management software to support user documentation updates;
3. documented the change management process based on the new software;
4. established a quarterly review of shared user accounts; and
5. implemented system notifications to notify certain staff of changes to user accounts.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2015015324 CIP-007-3a R6: R6.1; R6.4; R6.5 - OVERVIEW

SPP RE determined that URE did not implement technical and procedural mechanisms for monitoring security events on all Cyber Assets within the ESP as required by R6.1. Subsequent to SPP RE's determination, URE identified that it did not retain all logs for 90 calendar days as required by R6.4 or review logs of system events related to cyber security and maintain records documenting review of logs as required by R6.5. In two instances, URE failed to collect security event logs and failed to monitor for security events for approximately four months and one month, respectively. URE rebooted a switch, and all log events for approximately three months that had not been saved from the switch, other than critical warnings, were lost.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE's Cyber Assets reside within a physical access-controlled data center and behind a firewall. Where technically feasible, anti-virus and malware prevention tools are implemented on Cyber Assets located within URE's ESP. Access to Cyber Assets within the ESP is limited to only those individuals with authorized physical and/or electronic access rights. All personnel with authorized access to Cyber Assets have CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS is staffed 24/7. URE has 24-hour closed-circuit television monitoring of the PSP locations, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 16 months, from the first date certain logs were not monitored for security events, through the last date that a manual review of logs was not performed.

To mitigate this violation, URE:

1. reinstituted a manual log retention and review process;
2. implemented software for automated log collection, retention, alerting, and reporting for all in-scope Cyber Assets; and
3. updated procedures to include the new processes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014510 CIP-008-3 R1: R1.6 - OVERVIEW

SPP RE determined that although URE conducted exercises intended to test its Cyber Security Incident Response Plan (CSIRP), there were multiple years in which the evidence provided did not demonstrate that URE followed the necessary steps required by the URE CSIRP.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE did have a documented CSIRP in place. URE's CCAs resided within a physical access-controlled data center and behind a firewall. All personnel with authorized access to CCAs had CIP training and current PRAs. The area with CCAs used in real-time operations of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 24 months, from the date the CSIRP should have been tested, through the date URE performed and documented a full test of its CSIRP.

To mitigate this violation, URE:

1. performed a paper drill test of its CSIRP, including a step-by-step exercise of the CSIRP;
2. documented and distributed a summary of the CSIRP exercise to participants for comments;
3. revised the CSIRP; and

4. hired additional staff to monitor and manage CIP-related policies, procedures, and processes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014511 CIP-009-3 R2 - OVERVIEW

SPP RE determined that although URE conducted exercises intended to exercise its recovery plan, there were multiple years in which the evidence provided did not demonstrate that the specified response actions required by the recovery plan were followed.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. As a corrective control, URE could move operational control to standby assets and backup control centers, which would have allowed URE to remain operational in the event the primary control center was compromised. URE's CCAs were physically and electronically segregated, located behind a firewall, and requiring an authorized user name and password combination in order to gain access. All personnel with access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operations of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber incidents during the violation.

SPP RE determined the duration of the violation to be approximately 40 months, from the date of the deficient recovery plan exercise, through the date URE performed a recovery plan exercise that documented the followed response actions required by the recovery plan.

To mitigate this violation, URE:

1. assigned a CIP senior manager;
2. provided recovery plan training to energy management system personnel;
3. performed and documented an exercise of its recovery plan; and
4. scheduled the next annual recovery plan exercise.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. SPP RE considered URE's compliance history and determined that URE had one prior violation each of CIP-003 R6; CIP-004 R4; CIP-005 R1; CIP-006-3 R2.2; CIP-006-3c R1.6.1; and CIP-007 R2, R4, R5, and R6. URE had two prior violations each of CIP-007 R1; CIP-008 R1.6; and CIP-009 R2. SPP RE aggravated the penalty for these violations, as they were repeat noncompliance with the subject NERC Reliability Standards;
2. SPP RE considered URE's delay in submitting and implementing its Mitigation Plans an aggravating factor. URE submitted several Mitigation Plans at least 15 months after the Compliance Audit, some of which URE completed over 18 months after the Compliance Audit. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards to improve URE's compliance culture and increase its responsiveness;
3. URE had an internal compliance program (ICP) at the time of the violation, which SPP RE did not consider a mitigating factor because of the number of repeat violations and because URE's ICP did not address the various root causes of the violations. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards, which is designed to improve URE's compliance culture;
4. URE admitted to the violations;
5. URE did not receive cooperation credit because SPP RE experienced difficulty obtaining substantive updates from URE regarding its mitigation progress. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards to increase its responsiveness and improve its engagements with SPP RE. SPP RE will conduct a Compliance Audit of URE in 2017;
6. URE submitted a Self-Report after receiving a notice of Compliance Audit for one of its instances of noncompliance for SPP2015015324 CIP-007-3 R6.1, R6.4, and R6.5, therefore SPP RE did not apply mitigating credit for the Self-Report;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. one violation posed a minimal and not a serious or substantial risk to the reliability of the BPS, and 12 violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS, as described above;

9. URE agreed to "above and beyond" activities, which SPP RE considered as an offset to the proposed financial penalty. Under the Settlement Agreement, URE will complete the following activities:
    a. URE contracted with a vendor to evaluate its CIP ICP, covering CIP-002 through CIP-011 requirements relating to low and medium impact Bulk Electric System Cyber Systems;
    b. URE will implement substation physical perimeter security;
    c. URE will implement software to analyze firewall and router configurations for the purpose of identifying security vulnerabilities and deviations from URE security policies;
    d. URE contracted with a vendor that performed a targeted Cyber-Vulnerability Assessment (CVA). The vendor will also train URE network security staff on how to use the vulnerability assessment tool for future CVA testing;
    e. URE implemented a program to perform active vulnerability assessments of operating system assets within its ESP on a monthly basis;
    f. A URE employee completed ethical hacker training and received ethical hacker certification, which aids in the use of preventive and detective controls to identify vulnerabilities and exploits specific to checkpoint firewalls;
    g. Certain URE staff will attend industrial control systems cyber security training, which applies the use of preventive and detective controls to identify and respond to vulnerabilities and exploits specific to industrial control systems; and
    h. At least one URE analyst will complete certified ethical hacking training and receive certified ethical hacking certification, which aids in the use of preventive and detective controls to identify and respond to cyber vulnerabilities and exploits.
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of two hundred fifty thousand dollars ($250,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 15, 2017 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred fifty thousand dollars ($250,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Ron Ciesiel General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 614-3265 (501) 821-8726 – facsimile rciesiel.re@spp.org Joe Gertsch Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1672 (501) 821-8726 – facsimile jgertsch.re@spp.org SPP RE File Clerk Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1681 (501) 821-8726 – facsimile spprefileclerk.re@spp.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Alexander Kaplen* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile alexander.kaplen@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Alexander Kaplen

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline*
Senior Counsel and Director of Enforcement Oversight
Alexander Kaplen*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
alexander.kaplen@nerc.net

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

September 28, 2017

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement to resolve all outstanding issues arising from SERC's determination and findings of 59 total violations, including 50 violations of Critical Infrastructure Protection (CIP) Reliability Standards and 9 violations of the Operations and Planning NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE admits to the violations and agrees to the assessed penalty of five hundred thousand dollars ($500,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SERC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012661	CIP-002-3	R3	High/ Severe	CA	Serious	$500K
SERC2016015522	CIP-002-3	R4	Lower/ Severe	SR	Moderate	
SERC2013012662	CIP-003-3	R1; R1.3	Medium/ Severe	CA	Moderate	
SERC2013012663	CIP-003-3	R6	Lower/ Severe	CA	Moderate	
SERC2013012664	CIP-004-3	R2; R2.1	Medium/ Severe	CA	Moderate	
SERC2013012665	CIP-004-3	R3	Medium/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016016616	CIP-004-3	R3; R3.3	Medium/ Moderate	SR	Moderate	
SERC2016015515	CIP-004-3a	R3; R3.2	Medium/ Moderate	SR	Minimal	
SERC2013012666	CIP-004-3	R4	Lower/ Severe	CA	Moderate	
SERC2016015480	CIP-004-3a	R4; R4.2	Lower/ Moderate	SR	Minimal	
SERC2016016615	CIP-004-6	R5; R5.2	Medium/ Moderate	SR	Minimal	
SERC2017016813	CIP-004-6	R5; R5.4	Medium/ Lower	SR	Minimal	
SERC2013012667	CIP-005-3	R1; R1.1; R1.5	Medium/ Severe	CA	Serious	$500K
SERC2016016619	CIP-005-3a	R1	Medium/ Severe	SR	Moderate	
SERC2017017849	CIP-005-3a	R1; R1.1	Medium/ Severe	SR	Moderate	
SERC2013012668	CIP-005-3	R2; R2.2; R2.4	Medium/ Severe	CA	Serious	
SERC2016016620	CIP-005-3a	R2; R2.2	Medium/ Severe	SR	Moderate	
SERC2013012669	CIP-005-3	R4; R4.2; R4.3; R4.4	Medium/ Severe	CA	Moderate	
SERC2013012670	CIP-005-3	R5; R5.1; R5.2	Lower/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016015523	CIP-005-3a	R5; R5.1	Lower/ Severe	SR	Moderate	$500K
SERC2013012671	CIP-006-3a	R1; R1.2; R1.8	Medium/ Severe	CA	Moderate	
SERC2016015516	CIP-006-3c	R1; R1.6	Medium/ Severe	SR	Serious	
SERC2016015524	CIP-006-3c	R1; R1.8	Lower/ Severe	SR	Moderate	
SERC2016016603	CIP-006-6	R1; R1.3	Medium/ Severe	SR	Moderate	
SERC2013012678	CIP-006-3a	R2	Medium/ Severe	CA	Moderate	
SERC2016016606	CIP-006-6	R2; R2.1	Medium/ Severe	SR	Minimal	
SERC2016016611	CIP-006-6	R2; R2.2	Medium/ Severe	SR	Minimal	
SERC2017017812	CIP-006-6	R2; R2.2	Medium/ Severe	SR	Minimal	
SERC2013012681	CIP-007-3a	R2; R2.1; R2.2; R2.3	Medium/ Severe	CA	Moderate	
SERC2013012675	CIP-007-3a	R3; R3.1; R3.2	Lower/ Severe	CA	Serious	
SERC2013012676	CIP-007-3a	R4; R4.1	Medium/ Severe	CA	Minimal	
SERC2013012677	CIP-007-3a	R5; R5.1.2; R5.3	Lower/ Severe	CA	Moderate	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012680	CIP-007-3a	R6; R6.1	Lower/ Severe	CA	Minimal	
SERC2013012679	CIP-007-3a	R8; R8.2; R8.3	Lower/ Severe	CA	Moderate	
SERC2016015525	CIP-007-3a	R9	Lower/ Severe	SR	Moderate	
SERC2017017851	CIP-007-6	R2; R2.1	Medium/ Moderate	SR	Minimal	
SERC2016016614	CIP-007-6	R2; R2.2	Medium/ Lower	SR	Minimal	
SERC2016016609	CIP-007-6	R2; R2.3	Medium/ High	SR	Minimal	
SERC2017017811	CIP-007-6	R2; R2.4	Medium/ Severe	SR	Moderate	$500K
SERC2017017813	CIP-007-3a	R6; R6.1	Medium/ Severe	SR	Minimal	
SERC2016016605	CIP-007-6	R4; R4.4	Medium/ Lower	SR	Minimal	
SERC2017017854	CIP-007-3a	R5; R5.2.1	Lower/ Severe	SR	Moderate	
SERC2016016607	CIP-007-3a	R5; R5.3.3	Lower/ Severe	SR	Moderate	
SERC2016016608	CIP-007-6	R5; R5.5	Medium/ High	SR	Minimal	
SERC2016016610	CIP-007-6	R5; R5.7	Medium/ Severe	SR	Minimal	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2013012682	CIP-009-3	R1	Medium/ Severe	CA	Moderate	$500K
SERC2017017850	CIP-010-2	R1; R1.1	Medium/ Severe	SR	Minimal	
SERC2016016612	CIP-010-2	R1; R1.3	Medium/ Severe	SR	Moderate	
SERC2017017852	CIP-010-2	R1; R1.5	Medium/ Severe	SR	Moderate	
SERC2016016613	CIP-010-2	R2; R2.1	Medium/ Severe	SR	Moderate	
SERC2016015460	BAL-002-1	R4	Medium/ Severe	PDS	Minimal	
SERC2016016157	BAL-003-1.1	R2	Medium/ Severe	SR	Minimal	
SERC2016015526	FAC-014-2	R3	Medium/ Severe	SR	Minimal	
SERC2016015527	FAC-014-2	R4	Medium/ Severe	SR	Minimal	
SERC2017016808	PRC-002-2	R5; R5.3	Lower/ Severe	SR	Minimal	
SERC2016015697	PRC-023-3	R6	High/ Severe	SR	Minimal	
SERC2016015532	TPL-002-0b	R1; R1.3	High/ Lower	SR	Minimal	
SERC2016015533	TPL-003-0b	R1; R1.3	High/ Lower	SR	Minimal	

Violation(s) Determined and Discovery Method *SR = Self-Report / PDS = Periodic Data Submittal / CA = Compliance Audit						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
SERC2016015534	TPL-004-0a	R1; R1.3	Medium/ Lower	SR	Minimal	$500K

FACTS COMMON TO VIOLATIONS

During a Compliance Audit, SERC determined that URE had multiple violations of the CIP Reliability Standards. Following the Compliance Audit, URE's initial responses to SERC's requests for information (RFIs) were only partially responsive to the questions asked. SERC attempted to resolve the noncompliance with URE. URE provided SERC with draft Mitigation Plans a year after the audit, but did not submit formal plans until two years after the audit. SERC staff conducted multiple on-site visits in order to validate URE's completion of Mitigation Plan milestones and the completion of Mitigation Plans. Three years after the audit, URE submitted an additional series of Self-Reports covering violations of both Operations and Planning Reliability Standards and CIP Reliability Standards.

Due to the poor quality of the evidence provided to SERC staff during the on-site visits, SERC staff was only able to validate that URE completed one-fifth of its Mitigation Plans. SERC staff ended the last on-site visit early because of the significant and repeated difficulties the SERC on-site team had in verifying Mitigation Plan completion using the evidence that URE presented. As a result, SERC issued a Notice of Alleged Violation and required URE to submit new Mitigation Plans for the violations that SERC staff was unable to verify.

Shortly thereafter, SERC and URE agreed to URE's working with an external team of advisors to help it identify any additional cybersecurity risks, develop adequate Mitigation Plans to address the existing violations and any new violations, and provide sufficient evidence to demonstrate compliance. This team of advisors' work resulted in additional CIP Self-Reports and Operations and Planning Self-Reports.

SERC determined that, while the risk posed to the bulk power system (BPS) by the individual violations ranged from minimal to serious, the collective risk of the 59 violations posed a serious risk to the reliability of the BPS. URE's violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS primarily because of the lengthy duration of the unmitigated risk.

Critical Infrastructure Protection Violations

URE's violations of the CIP Reliability Standards posed a higher risk to the reliability of the BPS primarily because of the lengthy duration the violations went on without mitigation. As one example, URE's failures relating to identifying and documenting its Critical Cyber Assets (CCAs) could result in incomplete or inaccurate documentation of the Electronic Security Perimeter (ESP) and associated Cyber Assets, which could lead personnel to take incorrect actions based on outdated or missing information. There were also failures across the CIP standards relating to lack of awareness, engagement, and accountability for CIP compliance. URE did have some protections in place to protect the reliability of the BPS. Specifically, URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP for unusual activity.

SERC2013012661 CIP-002-3 R3 - OVERVIEW

SERC determined that URE failed to develop a list of CCAs that included all CCAs essential to the operation of the Critical Assets. Specifically, URE excluded eight assets comprising a virtual storage infrastructure that it failed to identify and document as CCAs that were essential to the operation of a Critical Asset.

The cause of this violation was inadequate processes and procedures to identify CIP assets.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to identify, document, and protect the devices as CCAs could have led to unauthorized access, data loss, or the failure of operator workstations, which could disrupt URE's situational awareness of the BPS. Several factors increased the risk of the violation. First, the vendor personnel in URE's CIP-004 violations, described below, had electronic access to the devices, but URE had not ensured that those individuals had completed cybersecurity training or had valid personnel risk assessments (PRAs), and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. URE had no means of ensuring the authenticity of the vendor personnel accessing the devices from outside the ESP, who were able to use a URE shared account to make changes to those devices remotely. Second, URE also did not provide any of the CIP-007 protections to the devices, and the management interface was outside of the ESP. Third, URE did not have a documented network asset backup procedure which could be used to recover the devices. Some factors provided some degree of protection. URE protected the connections inside the ESP and inside a Physical Security Perimeter (PSP). Also, while the misuse or failure of the devices could prevent

URE personnel from initially logging onto a workstation, it would not prevent URE personnel from continuing to use a workstation on which they had already been working.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed Critical Assets needed to support the Bulk Electric System (BES) and created the initial CIP asset list identifying BES Cyber Assets, Physical Access Control Systems (PACS), Protected Cyber Assets (PCAs), and Electronic Access Control or Monitoring Systems (EACMS), which was signed by the CIP senior manager;
2. Created an asset management process to address the identification and documentation of BES Cyber Systems and the underlying CIP Assets comprising the BES Cyber Systems;
3. Implemented a URE CIP asset classifications procedure;
4. Completed an annual review of all URE assets to ensure not only the proper classification of URE CIP Assets, but also a review of those that are not identified as CIP Assets; and
5. Conducted training on the new procedures and identification of CIP Assets generally.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015522 CIP-002-3 R4 - OVERVIEW

SERC determined that URE failed to approve the risk-based assessment methodology (RBAM), the list of Critical Assets, and the list of CCAs annually in one year.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual approval, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to annually approve the RBAM, Critical Asset list, and CCA list could have resulted in failures to document changes in the RBAM or failures to assess and document whether all relevant facilities or Cyber Assets should be identified as Critical Assets or CCAs. The risk of this violation was elevated by similar URE failures to review documentation annually in NERC Violation IDs SERC2016015523 (CIP-005-3 R5), SERC2016015524 (CIP-006-3 R1.8), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and

compliance with the CIP Standards. Nevertheless, this violation represented a failure to review documentation annually and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from the date the URE failed to annually approve its RBAM through when URE's CIP senior manager signed and approved the RBAM.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had its CIP senior manager approve the RBAM;
2. Created, as a part of a renewed focus on managing documentation, a relevant department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP program. Job descriptions for those staffing positions include references to their role in document management; and
3. In order to track and manage deadlines, had its new IT department build a document management database that tracks review dates and will trigger notifications for reviews and updates to business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012662 CIP-003-3 R1; R1.3 - OVERVIEW

SERC determined that URE failed to demonstrate that its senior manager annually reviewed and approved its cybersecurity policy after its creation for approximately five years.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual approval.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document the annual review and approval of the cybersecurity policy documents by the senior manager could result in URE personnel using an outdated version of the cybersecurity policy documents that did not adequately address current threats or the current state of URE's cybersecurity protections and procedures. Outdated cybersecurity policy documents could lengthen the period of time URE would need to respond to and recover from an emergency. Nevertheless, URE's cybersecurity policy documents are readily available to all personnel, and URE

requires employees to acknowledge the cybersecurity policy documents annually. In addition, contractors are required to acknowledge and to sign the cybersecurity policy documents annually.

SERC determined the duration of the violation to be approximately three years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Revised its administrative processes to require the CIP senior manager to approve, in writing, the policies relevant to URE's CIP Program. The policies are listed with the effective date for each, a statement from the CIP senior manager, and the date and signature of the CIP senior manager. This document will be part of the documentation URE reviews and approves annually; and
2. Had its CIP senior manager approve the cybersecurity policy.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012663 CIP-003-3 R6 - OVERVIEW

SERC determined that URE failed to provide evidence that it adequately documented changes to hardware components of certain CCAs pursuant to the requirements of its documented change control process. URE created change request documentation that had a generic change summary but did not specify the CCA hardware that was removed, redeployed, or returned to the vendor.

The cause of this violation was URE's inadequate change management process and controls.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement its documented change control process resulted in insufficient documentation of changes to CCA hardware components, which could lead to unauthorized changes to CCAs or the disposal of CCA hardware without following approved redeployment or disposal procedures, potentially resulting in the compromise of CCA information. Nevertheless, URE managed the redeployment of Cyber Assets and CCA hardware from the decommissioned site to the new site, and there was no third party involved. URE personnel were present with vendor personnel while CCA hardware was replaced.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Revised its Change Management processes and controls to require additional details regarding the move or replacement of hardware components. URE also enhanced its asset disposal process documentation similarly;
2. Implemented full change management processes and controls for all hardware replacements for these devices;
3. Had the URE compliance department provide training to the server administration department for using the change management process for all hardware replacements;
4. Revised a specific process document to specifically link URE's asset management system to the disposal manifest by using serial number as a common key to both processes;
5. Revised a specific process document to specifically include language for the disposal of certain equipment;
6. Provided training on the changes; and
7. Provided the historic documents showing that the devices were tracked and managed by URE during the move.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012664 CIP-004-3 R2; R2.1 - OVERVIEW

SERC determined URE failed to provide sufficient evidence to demonstrate that remote vendor personnel received cybersecurity training prior to receiving electronic access to four devices URE identified as CCAs, and did not identify the access by vendors as a specified circumstance for an exception.

The cause of this violation was URE's inadequate oversight and procedures relating to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that vendor personnel were trained on its cybersecurity training program could lead to poor security practices that could result in the compromise of the identified CCAs, including the energy management system (EMS), adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support

agreement with the vendor where the vendor personnel are to undergo stringent vetting, including criminal background check and identity verification. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Restricted external access by vendor support resources by programmatically disabling the vendor gateway. Vendor support resources can no longer access CCAs without URE's authorization;
2. Moved the URE server into the ESP;
3. Identified the three vendor resources who are allowed to access the URE equipment. These three resources have provided completed PRA certifications and security awareness training;
4. Had the vendor resources complete URE security awareness training;
5. Had the relevant URE supervisor inform the personnel on their team who manage the vendor gateway that only the three named vendor staff are allowed through the gateway to access the vendor equipment which URE owns; and
6. Implemented the capturing of audit logging from the vendor gateway. This allows staff to monitor and review all access by vendor support personnel.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012665 CIP-004-3 R3 - OVERVIEW

SERC determined that URE failed to document that PRAs of third-party vendors had occurred pursuant to CIP-004 prior to granting access to CCAs. The SERC audit team discovered that a third-party vendor had electronic access to four devices that URE had identified as CCAs. The vendor personnel had electronic access in order to provide remote support, but URE had not documented that the required PRAs had been performed prior to granting access.

The cause of this violation was URE's inadequate oversight and procedures related to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document that vendor personnel had completed PRAs meeting the requirements of CIP-004 R3 could lead to individuals with criminal backgrounds gaining access to and compromising identified CCAs, including the EMS, adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support agreement with the vendor where the vendor personnel are to undergo stringent vetting, including a criminal background check and identity verification. Based on information provided by the vendor, its background checks include drug testing, something that is not required by R3. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately five years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented the capturing of audit logging from the vendor gateway. This allows staff to monitor and review all access by vendor support personnel to the vendor management console;
2. Removed external access by vendor resources by turning off the support gateway. Vendor support resources can no longer access this data storage appliance without URE consent and subsequent enabling of the gateway to the management console;
3. Had the vendor provide certification of a PRA for local, dedicated vendor resources which complied with URE requirements;
4. Had the relevant URE supervisor inform the personnel on their team who manage the vendor gateway that only the three named vendor staff are allowed through the gateway to access the vendor equipment which URE owns; and
5. Negotiated with the vendor to provide local, dedicated vendor resources for ongoing vendor maintenance and support of these devices, thus implementing more controlled access. At least one dedicated vendor resource has completed URE's security awareness training and provided a PRA, and will thus be allowed access to provide maintenance and support as needed. No other vendor resources will be allowed access until such time as they are compliant with URE security policies and procedures.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016616 CIP-004-3 R3; R3.3 - OVERVIEW

SERC determined that URE failed to document that PRAs for contractor and service vendor personnel with authorized cyber or authorized unescorted physical access to CCAs occurred pursuant to CIP-004-3. The URE PRA program did not have established criteria to evaluate any identified criminal history. Instead, when a PRA produced criminal exceptions, the URE legal department reviewed the PRA on a case-by-case basis.

On some occasions, URE required a completed PRA certification form from the vendor or contractor for individuals assigned to work within the URE CIP environments in situations where the contractor or vendor could not or would not subject the individual to the URE PRA process. The URE PRA certification form asked if there was any adverse information found during the vendor or contractor's PRA, but URE did not establish or provide any criteria for what constituted this criteria. In the event that the contractor or vendor determined that adverse information existed, based on its own criteria, URE would require additional information and details in order to make decisions and document reasons for either proceeding with employment or declining to pursue employment.

URE conducted its extent-of-condition assessment to determine the scope of this violation; 5.1% of the total population of individuals with authorized access to CCAs went through the PRA process where the contractor or vendor company conducted the PRA and provided the certification to URE.

The cause of this violation was a deficient PRA process. URE did not have defined criteria for what constituted acceptable or unacceptable PRA results.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to document what constituted acceptable or unacceptable PRA results for a period of at least six years could result in inconsistent assessments of personnel being evaluated for authorized access to CCAs. In the case of some contractors or vendors, URE was wholly dependent on the content and quality of the third-party review and the third kicparty's identification of any adverse information, as defined by the third party. Nevertheless, URE reviewed and assessed PRA results in which a third party identified any adverse information when conducting its own PRA.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Obtained a redacted PRA or performed a PRA for all outside contractors and service vendors with ESP or PSP access;
2. Approved changes to the human resources (HR) onboarding for contractors process to require that, for contractors, URE will either perform the PRA itself through its own provider, or will obtain a redacted PRA from the contracting agency;
3. Completed training on the HR onboarding for contractors process with reading and signing by relevant staff in multiple departments.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016015515 CIP-004-3a R3; R3.2 - OVERVIEW

SERC determined that URE failed to update each PRA at least every seven years after the initial PRA. The URE compliance department received a completed PRA renewal for a contract security guard. Upon review, the compliance department employee discovered that the preceding PRA had expired seven years after the initial PRA was completed, resulting in a gap of 85 days where the contract security guard did not have a valid PRA and retained his or her authorized unescorted physical access rights to CCAs.

The cause of the violation was the URE employee tasked with managing the reports to identify pending PRA expirations at the 60-day mark failed to review the reports required by the URE procedure.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to update a PRA could have allowed an individual with a recent criminal history to retain and use their physical access permissions to tamper with or destroy CCAs, thereby affecting normal operations or the reliability of the BPS. Nevertheless, this violation was limited to a single security guard for 85 days. The security guard was in good standing with URE at the time of the violation, and remained so afterward. URE only uses contract security guards licensed by the state, and a part of that license requires that the state conduct PRAs on licensed individuals every two years.

SERC determined the duration of the violation to be approximately 85 days, from the date URE failed to update a contract security guard's PRA every seven years through when URE received an updated PRA for the contract security guard.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had its vendor and the subject contractor complete updated PRAs. No adverse information was found as a result of the PRAs;
2. Initiated an extent-of-condition review to determine the scope and cause of the failure, and determined that there were no other instances where it failed to update a PRA at least every seven years;
3. Implemented its PRA renewal for contractors procedure, which contains steps that are performed by HR to ensure that a new PRA is obtained prior to the expiration date or access will be terminated;
4. Made additional revisions stating that in all cases possible, URE will perform the PRA for contractors with PSP or ESP access itself, and that a redacted PRA can be accepted from a vendor if approved by URE compliance; and
5. Trained all staff affected by the procedure.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012666 CIP-004-3 R4 - OVERVIEW

SERC determined that URE failed to maintain a list of vendor personnel with authorized cyber access to CCAs or ensure that it properly maintained access lists for the vendor personnel. The SERC audit team discovered that third-party vendor personnel had electronic access to four devices that URE had identified as CCAs. The vendor personnel had electronic access to provide remote support. Nevertheless, URE failed to maintain a list of vendor personnel with access to the CCAs or to ensure that access lists for the vendor personnel with authorized cyber access to the CCAs were properly maintained.

The cause of this violation was URE's inadequate oversight and procedures relating to vendor personnel.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to maintain access lists of vendor personnel or ensure that access lists for vendor personnel were properly maintained could result in unauthorized individuals gaining access to and compromising identified CCAs, including the EMS, adversely affecting URE's situational awareness of and control over its portion of the BPS. Nevertheless, URE maintains a support

agreement with the vendor where the vendor personnel are to undergo stringent vetting, including a criminal background check and identity verification. When vendor personnel access the devices, they do so under the provisions of a support agreement.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE created a list of the approved vendor resources with authorization to access the CCAs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a BES Cyber System access review procedure. This procedure sets forth an access review process conducted by the compliance department, which includes a quarterly process for reviewing vendor support resource access to storage devices;
2. Executed its vendor access procedure;
3. Created a list of named, approved vendor resources who are authorized to provide on-site support on the devices through a shared account that is logged into by URE staff and with a login and password known only to URE staff;
4. Completed a review that its list of individuals with ESP or PSP access is complete and accurate and produced a complete listing of all individuals with access to BES Cyber Systems and an indication of access, as well as a list of shared accounts from the URE domain; and
5. Conducted the following training:
    a. The compliance department staff having responsibility for the contractors access list completed a read-and-sign review of the access list process;
    b. System administration staff completed a read-and-sign review of the vendor access procedure; and
    c. The staff from multiple departments having responsibility for the URE CIP Asset user access procedure completed a read-and-sign review.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015480 CIP-004-3a R4; R4.2 - OVERVIEW

SERC determined that on two occasions URE failed to revoke access to CCAs within seven calendar days for individuals who no longer required such access. URE identified each instance of noncompliance through recently implemented internal controls.

In the first instance, URE terminated a contractor due to the end of the contract obligations, not a for-cause termination. When an HR representative submitted the form to have the contractor's electronic access permissions revoked, he or she misspelled the contractor's last name, and URE eliminated access permissions for the incorrect user ID, which had been previously created as a result of a past request for access that again involved misspelling of the contractor's last name.

In the second instance, promoted an employee to a new role. The employee's manager requested revocation of existing electronic access permissions on the same day. However, due to a failure to create the proper work order within the required seven calendar days, URE did not revoke the electronic access permissions until 23 days after URE promoted the employee to a new role.

The cause of the violation was a human performance failure by URE personnel to follow the established access revocation procedures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to revoke access to CCAs could have allowed individuals to access CCAs without proper authorization and misuse, damage, or destroy CCAs to the detriment of the reliability of the BPS. Both involved individuals were in good standing with URE at the time of the occurrence. URE determined that the individuals had not used or accessed the relevant accounts after they were terminated or changed positions.

SERC determined the duration of the violation to be approximately ten months, from eight days after the contractor was terminated in the first instance of noncompliance through when URE revoked access permissions for the last individual involved in the violation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

First Instance:

1. Removed physical access and deleted the Virtual Machine (VM) used by the contractor to access the ESP. These actions removed access and prevented the user from accessing the ESP and entering any URE facility in order to log on directly to a system;

2. Submitted a domain account removal request to remove the terminated contractor's user account and virtual private network (VPN) access, and the account was removed. No VPN account existed;
3. Implemented URE's revocation process. This process defines the steps that URE follows to ensure that when a termination occurs, all user access is removed. As an additional step to verify that all access has been removed, a compliance analyst is required to verify and ensure that all access has been removed;
4. Trained all URE staff affected by the updated revocation process;
5. Generated new reports from URE's HR management system (HRMS) and IT management system no later than the first business day of the month for a monthly review; and
6. Held a training session related to the monthly CIP-related access reconciliation of the HRMS and IT management system reports for all members of URE's relevant department. This department has responsibility for completing the monthly tasks related to this CIP-related access reconciliation.

Second Instance:

1. Removed the subject employee's access to CCAs and protected Cyber Asset information;
2. Approved revisions to URE's revocation process to take all transferring employees down to a level of access common to all URE employees; and
3. Trained all URE management on the new processes.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016615 CIP-004-6 R5; R5.2 - OVERVIEW

SERC determined that URE failed to remove access to High Impact BES Cyber Systems prior to the end of the next calendar day after the date on which the need to remove access was determined. URE discovered that an employee who transferred to a different department did not have authorized electronic and authorized unescorted physical access permissions to the High Impact BES Cyber Systems and the associated BES Cyber Assets removed by the end of the next calendar day. URE removed the individual's access permissions upon discovery—one day later.

The cause of the violation was that the URE process requires a URE manager to approve all employee transfers. This approval within the Human Resources system triggers the subsequent access revocations. In this instance, the manager approved the workflow a day late, resulting in this violation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to revoke an individual's authorized electronic and authorized unescorted physical access by the end of the next calendar after access was no longer required could have allowed the individual to use his or her access permissions to degrade URE operations or negatively affect the BPS. Nevertheless, URE revoked the access one day after it should have revoked access, limiting the duration of the violation. The single employee at issue was current on cybersecurity training, had a valid PRA, and was in good standing with URE.

SERC determined the duration of the violation to be approximately 12 hours, from the day after authorized electronic and authorized unescorted physical access should have been revoked through when URE removed authorized electronic and authorized unescorted physical access.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Conducted an extent-of-condition assessment, reviewed previous transfers conducted within the past 90 days, and discovered no additional instances of noncompliance;
2. Terminated the remaining access for the employee;
3. Approved revisions to its transfers process requiring a compliance analyst to generate a second access report after access removals have been completed to ensure that all access was removed by the end of the next calendar day following the effective date or transition date for the transfer;
4. Approved revisions to its revocation process to take all transferring employees down to a level of access common to all URE employees; and
5. Trained all URE management on the new processes.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017016813 CIP-004-6 R5; R5.4 - OVERVIEW

SERC determined that URE failed to remove a non-shared user account for access to High Impact BES Cyber Assets for a terminated individual within 30 calendar days of the effective date of the

termination action. A URE employee resigned from URE on good terms to take a new position outside of URE. On the same day, URE took possession of the employee's card access badge and removed the employee's ability to gain physical access, took possession of the employee's laptop, eliminated the employee's domain account and VPN account, and revoked the employee's two-factor authentication access. These actions by URE effectively eliminated the ability of the employee to access any URE system, site, or Cyber Asset.

Approximately two months later, while conducting a quarterly access review, URE discovered that this former employee had an active user account on two BES Cyber Assets. URE did not revoke the employee's local user account on two servers.

The cause of this violation was insufficient training resulting in the human error of failing to delete the terminated individual's user account.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to revoke a terminated individual's user account could allow a malicious individual to access and use it in order to disrupt URE operations or create negative impacts to the BPS. Nevertheless, URE removed the terminated individual's ability to physically access any URE facilities and remotely access any URE systems on the last day of employment. URE's ESPs and the PSPs established by URE would thwart any access attempts by an outsider, and any internal threats by URE personnel would have to know the local user account password.

SERC determined the duration of the violation to be approximately five weeks, from the date 31 days after URE failed to revoke the terminated individual's non-shared user account through when URE revoked the terminated individual's non-shared user account.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Removed the terminated employee's physical access and his domain account;
2. Removed the remaining non-shared user account;
3. Approved a new user account removal procedure which includes all steps that a subject matter expert should use to remove accounts, verify that all accounts have been removed, and attach all evidence to a IT management system ticket;
4. Trained all relevant staff with a read-and-sign of the new user account removal procedure;

5. Improved the overall termination process by combining the involuntary termination and voluntary termination processes which ensure advance notification to staff responsible for removing access for both types of termination in its access termination process; and
6. Trained all staff affected by the updated access revocation terminations process with a read-and-sign of the process.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012667 CIP-005-3 R1; R1.1; R1.5 - OVERVIEW

SERC determined that URE failed to identify and document all access points to the ESP and failed to afford EACM devices all of the protective measures specified in CIP-005 R1.5.

The cause of this violation was URE's decision to configure a corporate firewall outside of the identified ESP that URE operated as if it were an ESP. URE did not identify this outer corporate firewall as an ESP and thus did not include it in its CIP program or provide it with the protections required by the CIP Standards.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to identify all access points to the ESP could result in inadequate protection of the access points and provide an opportunity for malicious individuals to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS. URE's failure to afford EACM devices all of the protections specified in CIP-005 R1.5 could result in vulnerabilities to the ESP going unaddressed and provide an opportunity for malicious individuals to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS.

Several factors increased the risk of the violation. The vendor personnel in URE's CIP-004 violations had electronic access to the devices which URE identified as CCAs, but URE had not ensured that those individuals had completed cybersecurity training or had valid PRAs, and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. URE had no means of ensuring the authenticity of the vendor personnel accessing the devices from outside the ESP, who were able to use a URE shared account to make changes to those devices remotely. Nevertheless, URE provided additional access control on the corporate firewalls which restricted the ports and services that had access to the CIP network. In addition, the vendor personnel whose authenticity were not verified at the ESP access points were operating under a service agreement with the vendor and underwent a background check prior to starting employment with the vendor. The

vendor personnel also had to use an individual username, password, and two-factor authentication token to gain access to the vendor gateway on URE's corporate network before accessing the devices.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

Issue 1: Electronic Access Points (EAPs)

1. Created, to correct the various devices that were incorrectly configured, a number of change requests to move the management consoles' IP addresses inside of the ESP. URE began moving these assets identified as EAP's into the ESP completely (removing any IP addresses outside the ESP). By placing these management interfaces into the ESP, the unidentified EAPs specified in the violation cease to exist;
2. Created an asset management process, including a new asset request process, to address the identification and documentation of BES Cyber Systems and the underlying CIP Assets comprising the BES Cyber Systems;
3. Updated and approved a document with steps to ensure that, for new devices, no ESP IP addresses will exist on a non-ESP asset, and that no non-ESP IP addresses existed on an ESP asset;
4. Implemented a URE CIP Asset classifications procedure, which is URE's process for identifying and correctly classifying URE CIP Assets. The URE CIP Asset classification document combined and replaced URE's BES Cyber Systems categorization process and URE CIP Asset classification procedure;
5. Completed an annual review of all URE assets to ensure not only the proper classification of URE CIP Assets, but also a review of those that are not identified as CIP Assets;
6. Conducted training on the new and revised procedures.

Issue 2: Ports and Services

1. Implemented a ports management process that sets forth the process for adding, updating, and decommissioning ports that have been determined to be needed for URE CIP Assets;

2. Implemented a ports and services database reconciliation procedure that details the procedure the administrator uses for reconciling the data with the ports and services database and conducting a monthly validation;
3. Made updates effective in CIP task templates (for asset new builds, asset changes, and asset decommissions) related to ports and services tasks. Notification of the updates was sent to the IT department email distribution the same day;
4. Completed a review of the listing of all ports in its ports and services database that contains the data for the open logical network accessible ports for all URE CIP Assets and their associated justifications, and the justifications for the ports undergoing testing were further updated to add the IT management system ticket for additional testing to determine if closure is possible;
5. Conducted training and distribution of information related to ensuring that only ports and services required for normal and emergency operations were enabled and proper justification of such ports;

Issue 3: Patch Management

1. Developed the final in-scope Cyber Asset software and patch source list. The patch source list was revised to make clarifications to patch sources and supplemental information;
2. Documented the patch management process in its CIP patch management process pursuant to CIP-007-5 R2;
3. Finalized a review of patch levels to ensure that patches on all URE CIP Assets were at the appropriate patch level;
4. Completed patching cycle;
5. Conducted training related to this violation and the mitigation steps;

Issue 4: Cyber Vulnerability Assessment (CVA)

1. Developed a CVA procedure;
2. Had relevant staff complete a read-and-sign of CVA procedure;
3. Held a kick-off meeting to discuss the upcoming CVA and the roles and responsibilities, with a make-up session, for representatives from relevant teams;
4. Completed its CVA; and

5. Shifted responsibility to conduct the annual CVA from one analyst in the compliance department to the entirety of a certain department to leverage the larger number of personnel and their focus on cybersecurity and thus ensure that the next CVA was conducted on time. URE also created an automated incident ticket to remind the relevant department when it is time to begin the CVA.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016619 CIP-005-3a R1 - OVERVIEW

SERC determined that URE failed to have all External Routable Connectivity go through an identified EAP.

The cause of this violation was a misinterpretation of the CIP Standard language. URE interpreted the CIP Standards and concluded that data traveling across an ESP to another ESP would not be in violation of the CIP Standards. In addition, URE determined that since it managed and routed the network traffic, the mingling of the CIP traffic with corporate traffic was not an issue or a compliance risk.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify and protect EAPs on the mixed trust infrastructure could have left Cyber Assets or BES Cyber Systems vulnerable to denial of service attacks and CIP data vulnerable to theft via attacks on the corporate network. URE's failure to identify and protect EAPs used to communicate between the two data centers could leave CIP data vulnerable to theft. Nevertheless, URE monitored the communication links to the corporate network with intrusion detection and prevention systems to detect and alert on traffic anomalies. URE encrypted all traffic between the two data centers, minimizing the risk that any intercepted data could be used for malicious purposes.

SERC determined the duration of the violation to be ongoing, from the date when URE implemented a mixed trust environment and did not identify the resulting EAPs to the ESPs through when URE is expected to complete its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide a network diagram depicting the ESP network and describing the functions of relevant devices;

2. Provide an update to SERC on the status of any Standard Drafting Team efforts that would allow the continued use of the ESP design in question;
3. Provide a draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design;
4. Complete trenching and laying of private fiber and install the new circuits at the facilities containing the ESPs;
5. Complete testing and move all corporate data traffic off of the mixed trust routers, which will resolve the mixed trust issue;
6. Update its network diagrams to identify any changes to BES Cyber Systems, EAPs, EACMS, PACS, and PCAs resulting from the resolution of the mixed trust issue;
7. Provide an update on the draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design; and
8. If a revised Standard allowing the use of the ESP design is not approved by FERC, URE will submit a revised Mitigation Plan to SERC that will document how and by what date URE will eliminate the ESP design. If the revised Standard is still in process but not yet approved, URE will consult with SERC on appropriate steps forward.

In addition, to mitigate this violation URE:

1. Approved CIP review process to provide required actions in the event that there is a creation or redesign of large-scale solutions related to the ESP;
2. Completed training on the CIP review process with a read-and-sign by relevant staff;
3. Executed a contract with vendor to install new circuits at the facilities containing the ESPs; and
4. Provided an update to SERC on circuit installation status.

Mitigation activities for this violation are still ongoing.

SERC2017017849 CIP-005-3a R1; R1.1 - OVERVIEW

SERC determined that URE failed to identify all access points to the ESP for all externally connected communication end points terminating at any device within the ESP. A user could move from the corporate network to the ESP network without having to authenticate through an ESP access point.

The cause of this violation was inadequate processes for URE to identify and prevent a dual-homed issue, with the resulting failure to identify an ESP access point, from occurring.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify the dual-homed scenario and resulting failure to identify an ESP access point could have allowed a malicious individual to move from the corporate network segment on the corporate side of the dual-homed device to the ESP network unchallenged by an appropriate access point. Nevertheless, the ESP and corporate, non-ESP network segments of these two Cyber Assets resided within a protected network segment, secured by a corporate firewall, which restricted access to a limited number of individuals. URE also utilizes an intrusion detection system with real-time alerting on any anomalous network activity.

SERC determined the duration of the violation to be approximately 18 months, from the date when URE implemented the dual-homed PCAs, thereby creating an ESP access point, through when URE removed the back-up functionality from the ESP interface, thereby removing the ESP access points.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the relevant department implement a control to review all interfaces before the asset is placed into production as part of its pre-production vulnerability assessment;
2. Had all relevant department staff complete training on this interface review control through a read-and-sign;
3. Had the relevant department institute a control performing an additional review of server builds to verify that the asset is not dual-homed and has the right network connection;
4. Had all relevant staff complete training on this server build review control through a read-and-sign; and
5. Completed additional training on acceptable network connectivity for BES Cyber Systems by relevant departments.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012668 CIP-005-3 R2; R2.2; R2.4 - OVERVIEW

SERC determined that URE failed to: (1) enable only the ports and services required for operations and for monitoring Cyber Assets within the ESP; and (2) implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party where external interactive access into the ESP was enabled. URE allowed full-range host-to-host communications to traverse the ESP access points, in effect failing to disable the ports and services not required for operations or monitoring of

Cyber Assets within the ESP. URE vendor personnel remotely connect through the dedicated vendor gateway and must authenticate at the gateway using a vendor username and password, as well as a two-factor authentication token. Nevertheless, when the vendor personnel access the devices, they use a URE shared account that URE personnel also use. URE does not verify the authenticity of the vendor personnel accessing the devices within the ESP at the access point as required by CIP-005 R2.4.

The cause of this violation was a lack of organizational processes and technical and procedural mechanisms for control of electronic access at all EAPs to the ESP.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to enable only those ports and services at the ESP access points that were required for operations and for monitoring Cyber Assets within the ESP increased the risk of unauthorized access though ports that were unnecessarily left enabled. Furthermore, URE's failure to verify the authenticity of the individuals accessing the devices at the ESP access points increased the risk of unauthorized access to CCAs. These failures could result in the compromise of CCAs, thereby reducing or eliminating URE's situational awareness over its portion of the BPS. The vendor personnel in URE's CIP-004 violations had electronic access to the devices, but URE had not ensured that those individuals had completed cybersecurity training or had valid PRAs, and had not ensured that the access rights of those individuals were being appropriately tracked by URE or the vendor. Nevertheless, URE provided additional access control on the corporate firewalls which restricted the ports and services that had access to the CIP network. In addition, the vendor personnel whose authenticity were not verified at the ESP access points were operating under a service agreement with the vendor and underwent a background check prior to starting employment with the vendor. The vendor personnel also had to use an individual username, password, and two-factor authentication token to gain access to the vendor gateway on URE's corporate network before accessing the devices.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Moved all relevant firewall rules from the corporate firewalls to the ESP firewalls, and the "default allow" status was changed to a "default deny" status on the ESP firewalls;
2. Reviewed the justifications of firewalls and initiated removal for any firewall access no longer needed;
3. Updated the network ESP technical documentation process to require that URE will use a "deny by default" rule and enable only needed ports and services when commissioning new firewalls.

Also updated the firewall deny by default procedure to detail how the "deny by default" requirement is implemented as firewalls are operated and managed;

4. Transferred management consoles from the corporate environment into the ESP, and the management console was readdressed so that all interfaces reside inside an ESP and no interfaces exist outside of an ESP;
5. Purchased and installed dedicated new hardware for use in the ESP;
6. Notified affected staff via email of the technicians allowed on-site to work on the consoles pending the completion of URE on-boarding requirements;
7. Changed the access on the gateway within the ESP to "Deny All", closing the gateway portal and removing the ability for technicians to access the gateway remotely;
8. Executed a storage administration vendor access procedure, which includes the required actions for maintenance and upgrades and specifically requires that they come on-site and be escorted by URE personnel;
9. Created a list of contractors with access to ESP storage to centralize the list of named, approved vendor resources who are authorized to provide on-site support on the consoles through a shared account that is logged into by URE staff and with a login and password known only to URE staff;
10. Updated URE policies and procedures so that the ESP network can only be logically accessed via the interactive access layer; and
11. Completed departmental read-and-sign training for all relevant staff.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016620 CIP-005-3a R2; R2.2 - OVERVIEW

URE did not, at all access points to the ESP, enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, and did not document the configuration of those ports and services. SERC determined that URE failed to require inbound and outbound access permissions at all EAPs for High Impact BES Cyber Systems and deny all other access by default.

The cause of this violation was a failure by URE staff to understand the operational risks and compliance impacts when reconfiguring ESPs.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to restrict ports and services on EAPs on the mixed trust infrastructure could have left BES Cyber Assets and BES Cyber Systems vulnerable to denial of service attacks and CIP data vulnerable to theft via attacks on the corporate network. URE's failure to restrict ports and services on EAPs used to communicate between the two ESPs could leave CIP data vulnerable to theft. Nevertheless, URE monitored the communication links to the corporate network with intrusion detection and prevention systems to detect and alert on traffic anomalies. URE encrypted all traffic between the two ESPs, minimizing the risk that any intercepted data could be used for malicious purposes.

SERC determined the duration of the violation to be approximately five years, from when URE implemented a mixed trust environment and did not enable only those ports and services required for operations and for monitoring Cyber Assets within the ESP on the resulting ESP access points without documenting the configuration of those ports and services, through when URE is expected to complete its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide a network diagram depicting the ESP network and describing the functions of relevant devices;
2. Provide an update to SERC on the status of any Standard Drafting Team efforts that would allow the continued use of the ESP design in question;
3. Provide a draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design;
4. Complete trenching and laying of private fiber and install the new circuits at the facilities containing the ESPs;
5. Complete testing and move all corporate data traffic off of the mixed trust routers, which will resolve the mixed trust issue;
6. Update its network diagrams to identify any changes to BES Cyber Systems, EAPs, EACMS, PACS, and PCAs resulting from the resolution of the mixed trust issue;
7. Provide an update on the draft plan to SERC detailing how URE would eliminate the ESP design if the CIP Standards are not modified to allow such an ESP design; and
8. If a revised Standard allowing the use of the ESP design is not approved by FERC, URE will submit a revised Mitigation Plan to SERC that will document how and by what date URE will

eliminate the ESP design. If the revised Standard is still in process but not yet approved, URE will consult with SERC on appropriate steps forward.

In addition, to mitigate this violation URE:

1. Approved a CIP review process to provide required actions in the event that there is a creation or redesign of large-scale solutions related to the ESP;
2. Completed training on the CIP review process with a read-and-sign by relevant staff;
3. Executed a contract with vendor to install new circuits at the facilities containing the ESPs; and
4. Provided an update to SERC on circuit installation status.

Mitigation activities for this violation are still ongoing.

SERC2013012669 CIP-005-3 R4; R4.2; R4.3; R4.4 - OVERVIEW

SERC determined that URE failed to perform an annual CVA on the access points to the ESP that: (1) disabled all ports and services that were not required for normal or emergency operations; (2) included the discovery of all ESP access points; and (3) provided documented evidence that a review of controls for default accounts, passwords, and network management community strings was completed.

The cause of this violation was URE did not have adequate documentation procedures relevant to the CVA.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to perform the annual CVA in accordance with the requirements of CIP-005 R4 could leave ESP access points in an insecure state, providing malicious individuals an opportunity to gain unauthorized electronic access to CCAs and thereby disrupt URE's situational awareness of the BPS. Nevertheless, URE subject matter experts reviewed the CVA results in order to confirm whether specific ports or services were required to be enabled, which could help identify any enabled ports and services that should be disabled. URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately six-and-a-half years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed a CVA procedure;
2. Had relevant personnel complete a read-and-sign of the CVA procedure;
3. Held a meeting to discuss the roles and responsibilities for an upcoming CVA;
4. Completed a CVA; and
5. Shifted responsibility of the CVA to ensure it is conducted on time.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012670 CIP-005-3 R5; R5.1; R5.2 - OVERVIEW

SERC determined that URE failed to ensure that all documentation required by CIP-005 reflected current configurations and processes as required by CIP-005 R5.1. SERC also determined that URE failed to update documentation required to support compliance with the requirements of CIP-005 within 90 calendar days of making modifications to the network or controls as required by CIP-005 R5.2.

The cause of this violation was URE's lack of a documented process to ensure compliance with the Standard, which allowed for human error and procedural breakdown.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that all documentation required by CIP-005 reflected current configurations and processes as required by CIP-005 R5.1 and to demonstrate that it reviewed all documentation and procedures required by CIP-005 at least annually could result in incomplete or inaccurate documentation of the ESP and associated Cyber Assets, which could lead personnel to take incorrect actions based on outdated or missing information. URE's failure to update documentation to reflect network changes within 90 days of the change as required by CIP-005 R5.2 could result in the misrepresentation of the network and ESP, which could result in misidentification of the Cyber Assets necessary for URE's situational awareness of the BPS and possibly impede or delay URE's ability to respond to or recover from an emergency. Furthermore, inaccurate drawings of the ESP and associated Cyber Assets could result in a failure by URE to identify all Cyber Assets within the ESP, including Cyber Assets that were introduced without authorization, and all access points to the ESP, which could provide unauthorized access to CCAs and other Cyber Assets.

Nevertheless, URE had a network-based intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of

unusual activity. In addition, URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately five-and-a-half years, from the date the audit period began through when URE updated its network diagrams.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Added revision history and cover sheet to the network diagram documenting the changes made to the network diagram and the dates those changes were made. In addition, URE began annually approving the network diagram;
2. Implemented a network ESP technical documentation process for documenting the ESP to include the network diagram, external routable communication paths, and inbound and outbound ESP access point rules;
3. Updated URE's change management process to include task templates used whenever a change impacted a CIP asset to update any CIP-related documentation that may have changed as part of that change request work, ensuring that any documentation gets reviewed and updated as part of the change request; and
4. Provided training related to this violation and mitigation on the network ESP technical documentation process and had a departmental read-and-sign.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015523 CIP-005-3a R5; R5.1 - OVERVIEW

SERC determined that URE failed to review at least nine documents in one annual CIP documentation review. URE discovered this violation while preparing for the implementation of CIP Version 5.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure it conducted the annual review, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct an annual review of its CIP-005-3 documents and procedures could have resulted in outdated configurations, documents, procedures, and processes around its ESPs and electronic access controls remaining in effect, possibly introducing gaps in the protections provided by the ESPs and electronic access controls. The risk of this violation was elevated

by similar URE failures to annually review documentation in NERC Violation IDs SERC2016015522 (CIP-002-3 R4), SERC2016015524 (CIP-006-3 R1.8), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and compliance with the CIP Standards. Nevertheless, this violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from the date URE failed to annually review the documents and procedures referenced in CIP-005-3 through when URE completed the annual review of its documentation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved the documentation required in CIP-005 R1, R2, and R3;
2. Created a department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP program; and
3. Built a document management database that tracks review dates and will trigger reviews and updates for business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012671 CIP-006-3a R1; R1.2; R1.8 - OVERVIEW

SERC determined that URE failed to: (1) identify all physical access points through each PSP; and (2) ensure the senior manager or delegate reviewed and approved its physical security plan annually.

The cause of this violation was inadequate processes and procedures.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to identify physical access points to the PSP could leave those physical access points without appropriate protections against unauthorized physical access. This could allow unauthorized individuals to gain physical access to CCAs, giving them the ability to damage, destroy, or misuse the CCAs, thereby reducing or eliminating URE's situational awareness of the BPS. In addition, URE's failure to have the senior manager or delegate approve the physical security plan and its failure to annually review the physical security plan could result in changes to the PSP going undocumented and indicates a weakness in URE's internal controls leading to an inconsistency in the

application of its CIP program, which could result in weaknesses in the physical protection of Critical Assets and CCAs.

Nevertheless, at the first location URE had deployed a card reader, door contact, and an exterior camera to protect against unauthorized access and log entry at the access point. At the second location, the first access point did not have a camera monitoring it but could only be opened from the inside and would alarm to a centralized alarm monitoring station upon opening. The second access point had a door contact that would alarm when opened and an interior camera for monitoring, while the third access point had a magnetic lock, card reader, and an exterior camera deployed. In addition, the physical security plan was reviewed by a specific manager in two prior consecutive years, indicating that URE personnel were aware of the need to review the physical security plan annually. The PSPs in question were also protected by fences and locked gates, limiting the ability of unauthorized individuals to gain physical access to the PSPs.

SERC determined the duration of the violation to be approximately 5 years and 11 months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Added the PSP access points identified as missing to URE's physical security plan, which was approved by the CIP senior manager;
2. Added a PSP access point section to the physical security maintenance and testing procedure, requiring performance of a visual inspection of the entire PSP to look for changes related to physical access points;
3. Improved the visual inspection process outlined in the physical security maintenance and testing procedure with a revision to the physical security inspection forms; and
4. Provided training on the physical security maintenance and testing procedure to the relevant team members with job functions related to the access point visual inspection and had those individuals complete a read-and-sign acknowledgement.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015516 CIP-006-3c R1; R1.6 - OVERVIEW

SERC determined that URE, in over 1,900 instances, failed to implement its visitor control program for visitors without authorized unescorted access to a PSP.

The cause of this violation was URE's failure to exercise sufficient oversight and conduct sufficient training to ensure adequate implementation of the URE visitor control program. URE failed to follow its visitor control program in a variety of ways, including failures to include visitor names or legible visitor names within the logbooks, failures to document the time that visitors entered and exited the PSP, and failures to document the identity of the escort for visitors within the PSP.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to implement its visitor control program on over 1,900 occasions could have allowed unauthorized personnel to gain physical access to CCAs and manipulate, disable, or destroy them to the detriment of the reliability of the BPS. Nevertheless, the PSPs in question are staffed with operations staff as well as security 24 hours a day, seven days a week and have closed circuit television feeds to the security console.

SERC determined the duration of the violation to be approximately two-and-a-half years, from the date of the earliest noted issue found by URE during its extent-of-condition review through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Dismissed the contracted security guard that failed to properly escort a visitor from working at URE;
2. Conducted a refresher escort training for all contracted security guards;
3. Delivered the updated URE training to all contracted security guards which included procedures for escorting non-authorized persons into the PSP;
4. Issued an order to all contract security guards, directing the proper procedure for logging visitors' entry and exit from certain parts of the PSP;
5. Issued an order to all contract security guards, directing the proper procedure for logging visitor's entry and exit from certain parts of the PSP other than the previous order; and
6. Implemented a new procedure for gathering and reviewing the visitor log book.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015524 CIP-006-3c R1; R1.8 - OVERVIEW

SERC determined that URE failed to implement its physical security plan's requirement to perform an annual review of its physical security plan. URE discovered this violation while preparing for the implementation of CIP Version 5.

The cause of this violation was URE's lack of adequate internal controls, such as reminders or alerts, to ensure that it conducted the annual review, and a lack of personnel resources.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct an annual review of the physical security plan could have resulted in outdated documentation of its PSPs and physical access controls, possibly introducing gaps in the protections provided by the PSPs and physical access controls. The risk of this violation was elevated by similar URE failures to annually review documentation in NERC Violation IDs SERC2016015522 (CIP-002-3 R4), SERC2016015523 (CIP-005-3 R5), and SERC2016015525 (CIP-007-3 R9). This widespread failure is indicative of weak internal controls around cybersecurity and compliance with the CIP Standards. Nevertheless, this violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately one month, from one day after URE failed to implement its physical security plan's requirement to annually review the physical security plan through when URE completed its annual review of the physical security plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved URE's physical security plan;
2. Created a department, in part, to manage processes and documentation for the IT department and to support quality control for URE's CIP Program; and
3. Built a document management database that tracks review dates and will trigger reviews and updates for business owners.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016603 CIP-006-6 R1; R1.3 - OVERVIEW

SERC determined that URE failed to utilize two different physical access controls to allow authorized individuals to have unescorted physical access into PSPs protecting High Impact BES Cyber Systems and

their associated EACMS and PCAs. Shared knowledge of a personal identification number (PIN) between the authorized individual and a system administrator rendered this physical access control insecure. URE determined that one of the two separate physical access controls it utilized to allow authorized unescorted physical access into relevant PSPs was not secure. The two physical access controls URE utilized were (1) a coded badge that an authorized individual possessed and (2) a personal identification number code that an authorized individual knew. However, when URE authorized unescorted physical access to an individual, one of two URE system administrators for the Physical Access Control System entered the PIN code that the authorized individual selected into the PACS. As a result, a system administrator knew the PIN code for any individual that he or she authorized to have unescorted physical access to the relevant PSP. The shared knowledge of each such PIN code between the authorized individual and a system administrator rendered this physical access control insecure.

The cause of this violation was a lack of understanding around this specific requirement and the need for the PIN to be secure to each individual authorized for unescorted physical access to the PSPs in question. URE's procedures did not ensure that each authorized individual entered their unique PIN into the PACS to avoid shared knowledge of the PIN.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that each authorized individual was the only person that knew their PIN code could have allowed an individual to obtain an authorized individual's badge and use the PIN code to gain unauthorized physical access to PSPs protecting High Impact BES Cyber Systems and take action to negatively impact the reliability of the BPS. Reducing the risk, only two URE system administrators entered the PIN codes for authorized individuals into the PACS, and both system administrators had authorized unescorted physical access to all URE PSPs. URE operators and control staff are present in PSPs 24 hours a day, 7 days a week, limiting the ability of an unauthorized individual to enter a PSP without being noticed. URE maintains on-site armed security staff that could be notified if an unauthorized individual was observed entering or exiting a PSP. URE security staff also monitors multiple camera feeds from all PSP access doors, allowing identification of any unauthorized individual.

SERC determined the duration of the violation to be approximately six months, from the date the standard became mandatory and enforceable through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Executed a physical access user management process to require that when receiving card key badges permitting access into a PSP, that the PIN must be entered by the individual receiving the badge;
2. Completed training for applicable staff with a read-and-sign of the physical access user management process;
3. Installed a separate key pad, which allows the individual receiving the badge to securely enter his or her PIN into the keypad, which is separate from the keyboard the administrator uses to create the badge; and
4. Conducted PSP obligations and responsibilities training, which included training on PIN creation and confidentiality for badge holders who have unescorted access into a PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012678 CIP-006-3a R2 - OVERVIEW

SERC determined that URE failed to afford all of the protective measures specified in CIP-007 R2 and R3 to Cyber Assets used to authorize access to the PSP or PACS devices. URE's process for ensuring that only those ports and services required for normal and emergency operations was documented but did not describe how to do this for PACS devices. Although URE reviewed the enabled and disabled ports and services on PACS devices, it did not document the resulting list of ports and services or the justification for why a specific port or service should be enabled or disabled. Without a documented list of the required ports and services for the PACS devices, URE relied on its subject matter experts to review the enabled ports and services based on their expertise, leaving room for subjective decisions and human error.

The SERC audit team also found that URE failed to afford the protective measures specified in CIP-007 R3 to the PACS devices. URE's security patch management program was documented but did not address the need for tracking, evaluating, testing, and installing applicable cybersecurity patches on PACS devices. In addition, URE did not assess some cybersecurity patches or upgrades for PACS devices within 30 days of the availability of the security patches or upgrades. A contributing factor to this failure was the fact that URE did not maintain a documented inventory of the third-party applications installed on PACS devices, making it difficult for URE to ensure that it tracked the availability of security patches and upgrades for each third-party application.

The cause of this violation was that URE lacked adequate procedures to document that it afforded the protective measures as specified by CIP-007 R2 and R3 to the PACS devices.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failures to describe in its procedures how to ensure that only the ports and services required for normal and emergency operations were enabled, to document the need for the assessment of security patches and upgrades for PACS devices, and to assess security patches and updates within 30 days of availability increased the risk of unauthorized electronic access to PACS devices through ports that should have been disabled or through vulnerabilities that were addressed in security patches or upgrades. A malicious individual with unauthorized electronic access to PACS devices could tamper with or disable the PACS devices, allowing unauthorized physical access to CCAs protected within the PSPs. Nevertheless, the PSPs in question were protected by fences and locked gates, limiting the ability of unauthorized individuals to gain physical access to the CCAs and other Cyber Assets within the PSPs.

SERC determined the duration of the violation to be approximately six years and two months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Moved, with the implementation of a CIP patch management process, all physical access controls under URE's standard process, which includes the process for evaluating, testing, and installing applicable security patches on all URE CIP Assets, including the physical access controls;
2. Maintained an inventory of software installed on CIP assets as part of its in-scope Cyber Asset software and patch source list;
3. Included all PACS devices in a patching cycle;
4. Finalized a process to bring the PACS devices into compliance with CIP-007-6 R1 and R2;
5. Addressed physical access controls under the ports management process and the ports and services justifications were updated for all PACS; and
6. Conducted IT cybersecurity patching training.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016016606 CIP-006-6 R2; R2.1 - OVERVIEW

SERC determined that URE failed to maintain continuous visitor escort for one of seven visitors in a group within a PSP protecting High Impact BES Cyber Systems and their associated EACMS and PCAs. During a tour, the escort discovered that one visitor was missing from the tour group. The escort immediately retraced the tour path, and found the missing visitor at the security desk in the foyer, just outside the PSP entrance. The missing individual left the group in order to take a phone call.

The cause of this violation was inadequate training leading to a human performance failure by the URE employee to escort visitors continuously while within the PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to maintain continuous escort of a visitor within a PSP could allow the visitor to physically access High Impact BES Cyber Systems and take action to negatively affect the reliability of the BPS. In this case, URE estimates that the time between the last known contact and the exit from the PSP was no more than five minutes. URE staff and armed security guards are within the building containing the PSP in question 24 hours a day, 7 days a week. URE documented the visitor's entry and exit from the PSP on the URE visitor logbook. All individuals on the tour were industry professionals from a compliance working group, and the visitor at issue was an employee at another entity. The visitor at issue abruptly exited the PSP and stood by the security guard station in the foyer until the rest of the tour group arrived in order to take a phone call.

URE conducted an extent-of-condition evaluation by reviewing the visitor logs and assessing the attendees and the assigned escort of all 41 tours conducted at its PSPs over the preceding quarter. URE then interviewed the escorts for all tours and confirmed via email response that at no point in any of the tours did any visitors leave the group or become unescorted.

SERC determined the duration of the violation to be approximately five minutes, from the time the visitor left the escorted tour group through when the URE escort found the visitor.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the escort locate the visitor and the visitor ultimately exited URE's PSP; and
2. Implemented a new training module that focuses on the obligations of those who have PSP access and what their obligations are respective to escorting visitors inside a PSP at URE.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016611 CIP-006-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to log entry and exit of a visitor to a PSP protecting High Impact BES Cyber Systems in five separate instances. URE initially identified this violation when the URE site manager was reviewing and reconciling visitor logs as a compliance check and discovered a single instance. URE identified the remaining four instances as part of an extent-of-condition evaluation conducted in response to a SERC request for information.

The cause of this violation was inadequate training leading to a human performance failure by URE escorts to follow the URE visitor control process for PSP access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document visitors into a nested PSP could make any forensic investigations following an incident difficult, because records of who was inside the interior nested PSP at any one time would not be readily available and accurate. Nevertheless, the interior PSP was within an access-controlled PSP, so the logs at the exterior PSP were complete, allowing identification of possible visitors to the interior PSP. In addition, URE operators and support staff work within the PSP at all times, allowing identification of visitors who may have entered the interior PSP. URE also maintains on-site armed security staff who work in the facility that contains both the exterior and interior PSPs, and the security staff are located at the front desk sign-in area and make periodic security rounds.

SERC determined the duration of the violation to be five different instances lasting between one minute and approximately one-and-a-half hours, from when URE escorted a visitor into the PSP without completely filling in the manual visitor logbook through when the escorted visitor exited the PSP.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Sent an email message to IT staff reminding them about the rules for documenting escorted visitor access to one of the interior (nested) PSPs;
2. Had a certain URE department implement a new visitor log book review procedure that requires a weekly review of visitor log books to examine the logbook entries for completeness and accuracy and to quickly detect any further violations of the requirement;
3. Completed training for the relevant URE staff responsible for reviewing the visitor log books with a read-and-sign of the visitor log book review procedure; and

4. Implemented a new training module that focuses on the obligations of those who have PSP access and what their obligations are respective to escorting visitors inside a PSP and logging visitor access to a PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017812 CIP-006-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to log entry and exit of a visitor to a PSP protecting High Impact BES Cyber Systems in two separate instances. URE conducted an extent-of-condition evaluation by comparing the prior 30 days of interior PSP logbooks to the exterior visitor logbooks. URE found no additional instances of noncompliance.

The cause of this violation was inadequate training leading to a failure of the escort to follow documented procedures around visitor escorting and interior PSPs nested within another PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document visitors into interior nested PSPs would make any forensic investigations or reviews following an incident difficult, since records of who was inside the interior nested PSP would not exist. Nevertheless, the nested PSPs are within an access-controlled PSP, and the logs at the exterior PSPs were complete. URE operators and support staff work within the exterior PSP at all times. URE also maintains on-site armed security staff who work at the front desk sign-in area and make periodic security rounds.

SERC determined the duration of the violation to be on two occasions, one lasting approximately three hours, and the other lasting approximately 19 minutes, from when the visitor entered the exterior PSP and subsequently advanced to the interior PSP without logging entry in the visitor logbook for the interior PSP through when the visitor exited the exterior PSP without logging the exit from the interior PSP.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Create a new post order for security staff to verbally instruct escorts of the requirement to log all visitor(s) into an interior PSP logbook whenever they are identified in the exterior PSP logbook as having a destination of an interior PSP;

2. Retrain necessary URE staff and security staff on the process of logging all visitors into and out of an interior PSP;
3. Update the weekly visitor log book review to add additional steps; and
4. Train relevant staff on the weekly visitor log book review.

In addition, to mitigate this violation, URE:

1. Confirmed via its records that the first visitor exited the exterior PSP;
2. Confirmed via its records that the second visitor exited the exterior PSP; and
3. Attached new signage at eye level to the front of each interior PSP access point door reminding escorts of the requirement to log visitors into an interior PSP.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012681 CIP-007-3a R2; R2.1; R2.2; R2.3 - OVERVIEW

SERC determined that URE failed to establish, document, and implement a process to ensure that it enabled only those ports and services required for normal and emergency operations and did not submit a request for a Technical Feasibility Exception (TFE).

The cause of this violation was that URE did not have a documented listing of ports and related justifications or a documented process. In addition, URE failed to submit requests for any needed TFEs.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to enable only the ports and services required for normal and emergency operations and its failure to document how to do so for all classes of Cyber Assets deployed within the ESP increased the risk of unauthorized electronic access to CCAs and other Cyber Assets within the ESP through ports and services that should have been disabled. A malicious individual with unauthorized electronic access to CCAs and other Cyber Assets within the ESP could tamper with or disable those devices, including those in the EMS, thereby disrupting URE's situational awareness of the BPS. In addition, URE's failure to document compensating measures or file a TFE for the Cyber Assets on which it was not technically feasible to disable unused ports and services could lead URE to overlook the ability to deploy newly developed compensating measures or new Cyber Assets that were capable of having unused ports and services disabled. Nevertheless, URE had a network-based

intrusion protection system, host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years and two months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a ports management process, which sets forth the process for adding, updating, and decommissioning ports that have been determined to be needed for URE CIP Assets;
2. Implemented a ports and services database reconciliation procedure that details the procedure the administrator uses for reconciling the data with the ports and services database and conducting a monthly validation. This procedure describes the process for enabling only those logical network accessible ports that are determined as needed through an asset's lifecycle;
3. Made updates effective in the CIP task templates (for asset new builds, asset changes, and asset decommissions) related to ports and services tasks;
4. Completed a review of the listing of all ports in its ports and services database, which contains the data for the open logical network accessible ports for all URE CIP Assets and their associated justifications, and further updated the justifications for the ports undergoing testing to determine if closure is possible; and
5. Conducted training and distribution of information related to ensuring that only ports and services required for normal and emergency operations were enabled and proper justification of such ports.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012675 CIP-007-3a R3; R3.1; R3.2 - OVERVIEW

SERC determined that URE failed to implement a security patch management program for tracking, evaluating, testing, and installing cybersecurity software patches for all Cyber Assets within the ESP. URE failed to document the assessment of security patches and security upgrades for third-party applications deployed on Cyber Assets within the ESP within 30 calendar days of the availability of such patches and upgrades.

The cause of this violation was a lack of adequate process documentation.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to assess security patches and updates within 30 calendar days of availability, and its subsequent failure to implement such security patches and updates or document compensating measures to mitigate risk exposure, left software on the affected CCAs and other Cyber Assets within the ESP vulnerable for an extended period, increasing the risk that a malicious individual could exploit known vulnerabilities that were addressed in security patches or upgrades. In addition, URE's failure to track, evaluate, test, and install applicable security patches and upgrades for third-party applications deployed on the CCAs and other Cyber Assets, and its failure to document compensating measures where it did not install such security patches or upgrades, could lead to vulnerable software going undetected, further increasing the time that a malicious individual could exploit known vulnerabilities. Nevertheless, URE had a network-based intrusion protection system, a host-based intrusion detection system, and security information and event management tools that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years and three months, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed the final in-scope Cyber Asset software and patch source list;
2. Documented the patch management process in URE's CIP patch management process pursuant to CIP-007-5 R2;
3. Finalized a review of patch levels to ensure that patches on all URE CIP Assets were at the appropriate patch level;
4. Completed the patching cycle; and
5. Conducted training related to this violation and the mitigation steps.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012676 CIP-007-3a R4; R4.1 - OVERVIEW

SERC determined that URE failed to document compensating measures to mitigate risk exposure for Cyber Assets within the ESP on which URE could not deploy anti-virus and malware prevention tools. The violation involved 12% of the total Cyber Assets and CCAs deployed within its ESPs that were purpose-built devices and were incapable of locally installing anti-virus and malware prevention tools.

The cause of this violation was inadequate process.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to document compensating measures or file a TFE for the Cyber Assets for which it was technically infeasible to install anti-virus software and malware prevention tools could lead URE to overlook the ability to deploy newly developed compensating measures or new Cyber Assets that were capable of installing such tools. Nevertheless, the Cyber Assets at issue were deployed within URE's ESP and were protected with an existing network-based intrusion protection system and host-based intrusion detection systems installed on other Cyber Assets within the ESP, and security information and event management tools that could alert URE in the event of unusual activity. These compensating measures, although not documented by URE in a TFE, significantly reduced the likelihood of a malware or virus infection on the Cyber Assets in question and would identify and limit the spread of such an infection on the ESP network.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a response process that sets forth URE's process of an overall defense-in-depth approach for mitigating malicious code under Version 5 of the CIP Standards. This process is consistent with the requirements of CIP Version 5, which does not require TFEs to be filed for devices not capable of supporting antivirus;
2. Approved the response process, which incorporated a requirement that, on a quarterly basis, each team perform a reconciliation against the asset database to ensure that all assets are being protected. Two IT teams are responsible for conducting a quarterly reconciliation; and
3. Conducted training on the revision to response process, which was accomplished with a read-and-sign.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012677 CIP-007-3a R5; R5.1.2; R5.3 - OVERVIEW

SERC determined that URE failed to: (1) implement the required password length, complexity, and annual change requirements as required by R5.3; and (2) document and implement a process to

capture user activity logs to create a sufficient audit trail of user account access activity as required by R5.1.2.

The cause of this violation was insufficient procedures.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Only a single Cyber Asset was technically unable to enforce the password length requirement, and only a few user accounts were not changed annually and were in an expired state that would require an immediate password change had they been accessed. In addition, URE had security systems in place that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. implemented a system access control process;
2. Implemented a security event monitoring process; and
3. Trained relevant personnel on the system access control process and security event monitoring process.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012680 CIP-007-3a R6; R6.1 - OVERVIEW

SERC determined that URE failed to show evidence of security status monitoring for all Cyber Assets within the ESP. URE documented the process to manage its automated security event management program implemented for Cyber Assets within the ESP, but the document failed to include the organizational process controls for Cyber Assets incapable of automated logging.

The cause of the violation was the lack of a process to configure, collect, monitor, and review all assets for security-related events and not submitting TFEs as appropriate.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation involved one Cyber Asset. URE performed an assessment of the Cyber Assets within the ESP and found that this was the only Cyber Asset incapable of having an automated tool

monitor system events related to cybersecurity. Additionally, URE had security systems that could alert URE in the event of unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented a security event monitoring process;
2. Reconciled, pursuant to its security event monitoring process, the list of assets being monitored against URE's CIP Asset List;
3. Added a task for configuring security event logging and alerting; and
4. Had certain personnel read and sign the security event monitoring process.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2013012679 CIP-007-3a R8; R8.2; R8.3 - OVERVIEW

SERC determined that URE failed to: (1) perform a review to verify that it enabled only ports and services required for operation of the Cyber Assets within the ESP; and (2) perform a review of controls for default accounts.

The cause of the violation was insufficient processes. URE's annual CVA of all Cyber Assets within the ESP did not adequately verify that only ports and services required for operations of the Cyber Assets within the ESP were enabled and did not demonstrate that it had conducted a review of controls for default accounts.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Nevertheless, URE had security measures in place that could alert URE in the event of unusual activity. Additionally URE had an active vulnerability scan that scanned the ESP network for unusual activity.

SERC determined the duration of the violation to be approximately six years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Developed a CVA procedure;
2. Had relevant personnel complete a read-and-sign of the CVA procedure;
3. Held a meeting to discuss the roles and responsibilities for an upcoming CVA;
4. Completed a CVA; and
5. Shifted responsibility for the CVA to ensure it is conducted on time.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2016015525 CIP-007-3a R9 - OVERVIEW

SERC determined that URE failed to review and update the documentation specified in Standard CIP-007-3a annually. URE depended on individuals within its compliance organization to be aware of the required annual CIP documentation reviews and start the process of preparing for and coordinating the annual review of documentation.

The cause of the violation was a lack of a documented process or controls to ensure the review and approval of documents in a timely fashion.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. This violation represented a failure to annually review documentation and would not have resulted in immediate operational impacts.

SERC determined the duration of the violation to be approximately two months, from one day after URE failed to annually review and update the documentation specified in CIP-007-3a through when URE completed its annual review and updated the documentation specified in CIP-007-3a.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed and approved documents that were due as required in CIP-007 R1-R7;
2. Created a department to manage process documentation and support quality control for URE's CIP Program; and
3. Built a document management database to track review dates and send notifications.

URE certified that it had completed all mitigation activities. SERC verified that URE had completed all mitigation activities.

SERC2017017851 CIP-007-6 R2; R2.1 - OVERVIEW

SERC determined that URE failed to identify itself as the patch source for custom-built software in its patch management process. URE identified multiple custom-built software applications installed on four URE BES Cyber Assets for which URE did not identify itself as the patching source.

The cause of the issue was inadequate procedures for identification of all patch sources.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE issued no security patches for these software applications since deployment. This violation affected only a few BES Cyber Assets and some internally developed software applications. URE utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP.

SERC determined the duration of the violation to be approximately eight months, from the date when the Standard became mandatory and enforceable, through when URE documented itself as the patch source for the custom-built software applications.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Provide an update to SERC on the status of its extent-of-condition review;
2. Complete an extent-of-condition review
3. Add software applications to URE's patch source list;
4. Complete patch assessments for the developed software applications;
5. Publish its patch management and vendor patch evaluations procedures;
6. Have relevant operations support staff complete training of the patch management and vendor patch evaluations procedure;
7. Update its CIP patch management process; and
8. Create email notifications of the CIP Patch management process.

Mitigation activities for this violation are still ongoing.

SERC2016016614 CIP-007-6 R2; R2.2 - OVERVIEW

SERC determined that URE failed to assess patches at least once every 35 days for applicability. The URE employee who had conducted the prior reviews of applicable security patches had accessed the vendor's website but navigated to the wrong page within the vendor website and thus did not find the patches.

The cause of this violation was inadequate training and procedures leading to human error. The URE employee responsible in two prior assessment periods did not go to the correct area of the vendor site to look for available patches.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The affected Cyber Assets were PCAs, and not BES Cyber Assets that were part of one of the High Impact BES Cyber Systems. Neither of the patches were cybersecurity-related. URE maintains a secured ESP within an established PSP.

SERC determined the duration of the violation to be approximately two weeks, from the date when URE had not evaluated the applicability of released patches from its identified patching sources within 35 days through when URE assessed the missed patches.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Evaluated all outstanding patch releases;
2. Had the applicable team sign up for automatic notifications of patches;
3. Approved revisions to the monthly patch verification procedure; and
4. Had specific departments complete training on the monthly patch management verification procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016609 CIP-007-6 R2; R2.3 - OVERVIEW

SERC determined that URE failed to apply applicable patches to 19 servers or create a dated Mitigation Plan within 35 days of the assessment date.

The cause of this violation was inadequate training and procedures leading to human error. The patching owner failed to follow the documented process and apply the patches or create a dated Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. In two instances, URE decommissioned an impacted Cyber Asset or removed impacted software to mitigate identified vulnerabilities. In addition, URE had disabled the software prior to its late removal. In total, the violation impacted approximately three percent of URE BES Cyber Assets. URE protected the Cyber Assets at issue within establish ESPs and PSPs, both with real-time monitoring and alerting. URE monitors for any changes to Cyber Asset configurations, and any unapproved changes generate immediate alerts. URE experienced no cybersecurity Incidents during the violation.

SERC determined the duration of the violation to be approximately two months, from the date the when URE exceeded 35 days between the assessment of security patches without applying the applicable patches or creating a dated Mitigation Plan through when URE decommissioned the BES Cyber Asset.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Applied the patches to the relevant servers;
2. Removed a server from the ESP network;
3. Uninstalled system management software;
4. Demonstrated the patching process has been correctly followed;
5. Added personnel to the server administration department;
6. Updated the CIP patch management process;
7. Conducted training related to updates to the patch management process;
8. Approved revisions to the monthly patch verification procedure; and
9. Trained multiple departments on the monthly patch verification procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017811 CIP-007-6 R2; R2.4 - OVERVIEW

SERC determined that URE failed to obtain the approval of the CIP senior manager or delegate to extend the completion date of a mitigation plan created pursuant to CIP-007-6 R2.3 before the timeframe for the original mitigation expired.

The cause of the violation was a failure to implement appropriate internal controls to ensure URE completed mitigation plans by the due date or obtained CIP senior manager (or delegate) approval of extensions to mitigation plan completion dates if required.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement a security patch mitigation plan impacting approximately 14% of the total URE Cyber Assets within the approved timeframe or obtain approval for an extension of the mitigation plan could have resulted in URE overlooking the implementation of the security patch, allowing a security vulnerability to remain on its systems for an extended period. Nevertheless, the actions URE put in place to mitigate the vulnerabilities addressed by the security patch have remained in place since the mitigation plan was documented by URE. URE had a defense-in-depth security strategy, which included firewalls with port restrictions and deny-by-default access rules and an intrusion detection system with alerting enabled. All URE CIP Cyber Assets are within a secured ESP with real-time alerting and monitoring.

SERC determined the duration of the violation to be approximately six days, from the day after the initial security patch mitigation plan expired without URE applying the security patch or approving an extension to the mitigation plan through when the extension to the mitigation plan completion date was approved by the CIP senior manager's delegate.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Had the applicable personnel approve an extension to the patch mitigation plan;
2. Set reminders for mitigation plan due dates;
3. Built a spreadsheet to track all patch mitigation plans;
4. Trained relevant staff on the patch mitigation plan controls; and
5. Made a notification to all relevant staff reminding staff responsible for CIP patching of how to manage their patching mitigation plans.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017813 CIP-007-3a R6; R6.1 - OVERVIEW

SERC determined that URE failed to log events at the BES Cyber System level (per BES Cyber System capability) or at the Cyber Asset level (per Cyber Asset capability) for identification of, and after-the-fact investigations of, cybersecurity Incidents. This violation involved two PCAs.

The cause of the violation was URE's product vendor's lack of awareness of the capabilities of a specific type of PCA.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to log events on the two PCAs could have hindered or prevented discovery of cybersecurity Incidents, or caused delays in the investigations of identified cybersecurity Incidents. Nevertheless, the two PCAs involved do not have any direct impact on URE operations or the BPS. URE uses these two PCAs to scan the network within the ESP for any new Cyber Assets. URE also utilizes an intrusion detection system with real-time alerting for any anomalous network activity. URE secures all Cyber Assets, including these two PCAs, within a defined ESP. Finally, after discovery of this capability to retain logs, URE was able to go back and review all logs dating back six months. URE found nothing suspicious in the logs that it was able to review.

SERC determined the duration of the violation to be approximately nine months, from the date URE put the PCAs into production without monitoring system events related to cybersecurity through when URE began pulling and retaining logs from the two PCAs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed an extent-of-condition review;
2. Obtained and reviewed logs for a specific device
3. Began frequently pulling and reviewing logs
4. Updated the security event log review procedure; and
5. Had the relevant department complete a read-and-sign of the updated event log review procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016605 CIP-007-6 R4; R4.4 - OVERVIEW

SERC determined that URE failed to review a sample of logged events in its automated security information and event management (SIEM) enterprise tool every 15 days to identify undetected cybersecurity Incidents on High Impact BES Cyber Systems and their associated EACMS and PCAs.

The cause of the violation was a failure to follow URE's procedure and lack of procedural controls.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to review and assess sample logs every 15 days could allow new or previously unidentified cybersecurity Incidents to go unrecognized for an extended time, delaying action to address the risk posed by a cybersecurity Incident. Nevertheless, URE was four days late in reviewing the log samples and did not identify any undetected cybersecurity Incidents in that review. URE also uses the automated SIEM tool for alerting for possible cybersecurity Incidents.

SERC determined the duration of the violation to be approximately four days, from the date a day after when URE should have conducted the 15-day assessment of event logs through when URE conducted the review of event logs.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reviewed the log upon discovery of the issue;
2. Created an automated recurring incident ticket that is automatically generated on a weekly basis;
3. Updated its security event log review procedure; and
4. Completed training for staff responsible for performing the CIP weekly log review procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017854 CIP-007-3a R5; R5.2.1 - OVERVIEW

SERC determined that in two instances URE failed to change passwords on administrator, shared, and other generic accounts prior to putting them into service in two separate instances when it could not remove, disable, or rename such accounts.

The cause of the first instance of the violation was a URE decision not to change the password as required, due to what URE deemed to be an unacceptable risk of opening up remote access and a lack of awareness of alternative options. The cause of the second instance was a failure of URE staff to follow the internal procedures, which require URE to change default accounts prior to installation.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's decision not to change default account passwords on certain Cyber Assets and its failure to explore possible work-arounds could have allowed a malicious actor to use well-known and widely distributed passwords to gain access to Cyber Assets within the URE network and thereby negatively affect URE operations or BPS reliability. Nevertheless, in the first instance, URE sought to reduce risk to the BPS by preventing remote access to the affected Cyber Assets. The second instance involved only two Cyber Assets. URE also utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately two years, from the date URE began deploying the Cyber Assets with default passwords installed through when URE changed the last default passwords on the Cyber Assets.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. For each new asset reviewed in the asset review meeting, gather information to capture if the asset has any default accounts and/or passwords;
2. Retrain relevant staff on the requirements of the system access control process;
3. Complete its extent-of-condition review;
4. Request and receive a position solution from the vendor to allow the password on a device to be changed without enabling remote access to the device;
5. Create an automated incident to notify the team when the next password change for a specific device is due;
6. Complete all troubleshooting with the vendor and testing;
7. Change the default password to the device on all machines that are CIP devices and have the agent installed;
8. Change the default passwords for multiple appliances; and

9. Create an automated notification to notify the team when the next password changes for the devices are due.

Mitigation activities for this violation are still ongoing.

SERC2016016607 CIP-007-3a R5; R5.3.3 - OVERVIEW

SERC determined that URE in three instances failed to enforce password changes technically or procedurally or enforce an obligation to change the password at least once every 15 calendar months for High Impact BES Cyber Systems and their associated EACMS, PACS, and PCAs.

The cause of the violation was a combination of inadequate controls and failure to follow URE's process requiring the change of passwords every 15 months.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to change passwords on an annual basis pursuant to CIP-007-3a R5.3.3 and at least every 15 months pursuant to CIP-007-6 R5.6 could have allowed malicious actors more time to guess or otherwise discover passwords. URE's failure to maintain evidence regarding the last password change for the Cyber Assets in the second instance of noncompliance increased the risk of the violation because URE had no evidence that it had ever changed those passwords, potentially leaving them vulnerable to guessing attacks for an extended period. Nevertheless, URE attested that all passwords in service in the three instances of noncompliance were sufficiently complex and at least eight characters in length, increasing the difficulty of guessing the passwords. In the first and second instances of noncompliance, 17 URE employees knew or could access these passwords, while in the third instance of noncompliance, only eight system administrators knew and could access this password.

SERC determined the duration of the violation to be approximately two years, from when URE should have had evidence of its compliance with CIP-007-3a through when URE changed the last password at issue in this violation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Changed relevant passwords;
2. Set up an automated incident ticket for the applicable accounts;
3. Revised the system access control procedure document;
4. Notified the relevant departments of the revisions to the system access control procedures;

5. Approved the assets and applications system access control revisions to the procedure document; and
6. Trained the relevant department on changes to the system access control procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016608 CIP-007-6 R5; R5.5 - OVERVIEW

SERC determined that URE failed to enforce the required password complexity on a device capable of supporting a password of at least eight characters and instead only used a password that was seven characters in length. A URE staff member scheduled a two-hour system outage in order to change its database account passwords after an employee transfer. After generating a random password to meet complexity requirements, the URE staff member inadvertently copied and pasted only seven of the eight-character password into the configuration files. Since the system masks the password, the URE staff member could not tell the error occurred. As an internal control as well as a programmatic password control, the URE staff member was required to paste the password into a database where a running script validated password compliance for complexity and length. In this instance, the script identified the password was seven characters instead of eight.

Security event logging was non-functional during the outage. Therefore due to the risk of possible reliability impacts due to an unplanned extended outage affecting its functions, URE staff decided not to extend the outage to make the necessary updates and scheduled a second system outage 15 hours later to update the password to the appropriate length.

The cause of this violation was insufficient training resulting in human error of placing a noncompliant password into the configuration files.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to have a password that met the length requirements could make it easier for a malicious actor to determine the password. Nevertheless, the noncompliant password was only in service for approximately 15 hours, and URE knew of the issue and scheduled a second outage to update the password to the appropriate length for the next day. Only two URE employees knew that a deficient password was in service, and only seven additional URE employees had access to the location where the password was stored.

SERC determined the duration of the violation to be approximately 15 hours, from when URE started operating with a database account password that was noncompliant through when URE resumed operations with a database account password that met the password length requirements.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Changed the password for the relevant database;
2. Updated procedures to clarify the password composition requirements; and
3. Notified the relevant departments of the password and procedure changes.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2016016610 CIP-007-6 R5; R5.7 - OVERVIEW

SERC determined that URE: (1) failed to limit the number of unsuccessful authentication attempts or generate alerts after reaching a threshold of unsuccessful authentication attempts for ten Cyber Assets because doing so was not technically feasible; and (2) did not request a TFE for those Cyber Assets.

The cause of the violation was a lack of sufficient process for requesting a TFE when limiting the number of unsuccessful authentication attempts or generating alerts after reaching a threshold of unsuccessful authentication attempts was not technically feasible.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to request a TFE when limiting the number of unsuccessful authentication attempts or generating alerts after reaching a threshold of unsuccessful authentication attempts was not technically feasible could have resulted in URE not implementing compensating measures to prevent a malicious actor from gaining unauthorized access through a password guessing attack or attempting to lock out an account through repeated authentication attempts. Nevertheless, although URE did not request a TFE as of the date of mandatory compliance, URE provided two attestations confirming that all compensating measures in the TFE that URE submitted to mitigate this violation had been in place since the time the Cyber Assets were placed into production. In addition, this violation only affected ten URE Cyber Assets that were protected within an ESP and PSP.

SERC determined the duration of the violation to be approximately five months, from the date the standard became mandatory and enforceable through when URE added the Cyber Assets to an existing CIP-007-6 R5.7 TFE.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Submitted a TFE for the devices which could not meet CIP-007-6 R5.7;
2. Approved a CIP asset classifications procedure;
3. Had relevant staff complete training on the CIP asset classification procedure;
4. Published its TFE procedure; and
5. Had relevant staff complete training on the TFE procedure.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2013012682 CIP-009-3 R1 - OVERVIEW

SERC determined that URE failed to document recovery procedures adequately for all CCAs. The URE recovery plans only included discussion of common assets, workstations, consoles, and services but did not address other deployed CCAs within the ESP and did not provide sufficient detail on how to recover all classes of CCAs.

The cause of the violation was insufficient process and documentation. URE did not create recovery plans for CCAs that: (1) provided adequate information on how to recover all CCAs, (2) specified the required actions in response to conditions of varying duration and severity that would activate the recovery plan, or (3) defined the roles and responsibilities of responders.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to create adequate recovery plans for CCAs could delay the recovery of CCAs in the event that they became non-functional, thereby impairing URE's situational awareness of its portion of the BPS. Nevertheless, URE had high-level business continuity and restoration plans that could be used to assist in the recovery of CCAs. URE's subject matter experts likely had the technical expertise to recover CCAs in the event that they became non-functional, and URE had no need to recover CCAs during the period covered by the audit.

SERC determined the duration of the violation to be approximately five and-a-half years from the date the audit period began, through when URE implemented a revised BES Cyber Systems recovery plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Implemented its BES Cyber Systems recovery plan pursuant to CIP-009-5 R1;

2. Held BES Cyber System recovery plan training for certain personnel;
3. Approved a new version of the BES Cyber System recovery plan; and
4. Conducted additional training on the BES Cyber System recovery plan.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2017017850 CIP-010-2 R1; R1.1 - OVERVIEW

SERC determined that URE failed to document all installed software on its baseline configurations in two instances.

The cause of the violation was a combination of insufficient training and insufficient internal controls to check and confirm baseline creation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to include custom software applications on the baseline for BES Cyber Assets and its omission of one BES Cyber Asset from a baseline entirely could have allowed undocumented changes to the baseline to go unnoticed and uninvestigated, potentially resulting in degradation of URE operations or the reliability of the BPS. Nevertheless, URE knew of custom-built software applications in the first instance and it required Active Directory access for logins, reducing the potential threat. URE was also able to provide evidence that it had tested the custom-built software when changes occurred, and that it periodically updated the software and tested it. One of the software applications was determined unneeded and unused since before the standard became mandatory and enforceable. For the second instance, URE omitted a single BES Cyber Asset from its baseline documentation for a period of approximately 10 months. URE also utilizes an intrusion detection system with real-time alerting for any anomalous network activity. URE secures all Cyber Assets within a defined ESP.

SERC determined the duration of the violation to be approximately ten months, from when the Standard became mandatory and enforceable through when URE completed documenting the last software application on its baseline documentation.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Train relevant staff on the review process for checking and resolving issues with assets;
2. Complete training on baselining custom software applications for relevant staff;

3. Complete an extent-of-condition review;
4. Uninstall the software application that was not in use from the servers on which it was installed;
5. Update the baseline to capture the remaining software applications;
6. Reconfigure the automatic baseline collector for the missing Cyber Asset and collect the baseline configuration; and
7. Implement controls that include checking and resolving issues with assets.

Mitigation activities for this violation are still ongoing.

SERC2016016612 CIP-010-2 R1; R1.3 - OVERVIEW

SERC determined that URE failed to update the baseline configuration as necessary within 30 calendar days of completing the change for High Impact BES Cyber Systems and their associated PACs that deviated from the existing baseline configuration.

The cause of the violation was insufficient procedures and training resulting in the human performance failure of not following the document processes for updating baseline configurations within 30 days of the change.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to update its baseline configuration for High Impact BES Cyber Systems and associated PCAs within 30 days could have permitted stale documentation around configurations and versions of software to influence decisions that URE would make, potentially affecting URE's operations and security posture. The risk was elevated because the URE baseline owner responsible for baseline updates pursuant to CIP-010-2 R2.1 was not monitoring the automated tool that identifies changes to baseline configurations (see NERC Violation ID SERC2016016613). Nevertheless, this violation only affected approximately 1% of the total Cyber Assets. All changes at issue went through the appropriate change management process and were tested and approved. The Cyber Assets involved in this violation are mostly purpose-built with infrequent changes necessary. The Cyber Assets involved in this violation resided within secured PSPs and ESPs, both with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately five months, from the date 31 days after a change that deviated from the existing baseline configuration without URE updating the baseline configuration through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reconciled all outstanding changes to their respective baselines and promoted as appropriate for the device;
2. Implemented baseline exception reporting and escalation with asset exceptions report;
3. Revised the baseline configuration management process; and
4. Conducted training on the revised process for baseline owners.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

SERC2017017852 CIP-010-2 R1; R1.5 - OVERVIEW

SERC determined that URE, in three instances, failed to document test results and did not test all changes to High Impact BES Cyber Systems in a test environment or a production environment in such a way to minimize adverse effects prior to implementing a change in the production environment.

The cause of this violation was a lack of training on the change management procedures in instances one and three, and a failure by URE to understand and properly investigate the potential consequences of a change in instance two.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to conduct testing prior to implementing a change in the production environment and its failure to retain test results of changes could result in operational impacts and make assessment of negative impacts difficult. Nevertheless, URE had internal controls in place that identified these failures within approximately a month at the longest, allowing URE to address any identified problems in a timely manner. URE utilizes an intrusion detection system with real-time alerting on any anomalous network activity. URE secures all Cyber Assets within a defined ESP. URE did not experience any adverse effects or find any adverse impacts to its CIP-005 and CIP-007 cybersecurity controls as a result of the violation.

SERC determined the duration of the violation to be approximately four months, from when URE patched assets without retaining documentation of testing in the first instance through when URE discovered the third instance in which it did not document specific testing and save the results.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE will:

1. Complete its extent-of-condition review;
2. Make process and documentation updates to the baseline configuration change management procedure/process;
3. Train all relevant staff on the updated procedure and process;
4. Implement the change ticket review for CIP assets procedure; and
5. Complete training for relevant staff on the change ticket review for CIP assets procedure.

Mitigation activities for this violation are still ongoing.

SERC2016016613 CIP-010-2 R2; R2.1 - OVERVIEW

SERC determined that URE failed to monitor, at least once every 35 calendar days, for changes to the baseline configuration on High Impact BES Cyber Systems and their associated EACMS and PCAs. This violation involved the same Cyber Assets at issue in a CIP-010-2 R1.3 violation (NERC ID SERC2016016612). URE learned that the automated tool it used to conduct the automated comparison was identifying the change between the configuration running in the production environment and the documented configuration in the baseline, but the URE baseline owner responsible for baseline updates was not monitoring the application reporting tool dashboard for exceptions.

The cause of the violation was a combination of insufficient controls and human performance failure. URE did not have adequate controls in place to identify assets as the monitoring window was closing and did not notify and escalate to the appropriate staff for resolution. URE staff did not follow the established process and conduct the manual review of the dashboard showing changes to the baseline configurations.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor for changes to the baseline configuration running in production when compared to the documented baseline could have resulted in URE not noticing or resolving changes that had been made, either appropriate or malicious, possibly leading to operational impacts. Nevertheless, this violation only affected approximately 5% of the total Cyber Assets. All changes at issue went through the appropriate change management process and were tested and approved. The Cyber Assets involved in this violation are mostly purpose-built with infrequent changes necessary. The Cyber Assets involved in this violation resided within secured PSPs and ESPs, both with real-time monitoring and alerting.

SERC determined the duration of the violation to be approximately seven months, from the date 36 days after a change that deviated from the existing baseline configuration without URE investigating the change through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Reconciled outstanding changes to their respective baselines, promoted, and where applicable, manually monitored;
2. Implemented CIP baseline exceptions and CIP baseline manual asset monitoring reports;
3. Revised the baseline configuration management process; and
4. Conducted training on the revised process for baseline owners.

URE certified that it had completed all mitigation activities. SERC has not yet verified that URE has completed all mitigation activities.

Operations and Planning Violations

URE's violations of the Operations and Planning Reliability Standards posed minimal risk to the reliability of the BPS. URE had protections in place that prevented elevated risk to the BPS, and no harm is known to have occurred from any of these violations. Specifically, URE would have responded to frequency deviations with a larger change in generation than it was required to provide. The larger contribution would tend to reduce the excursion, reduce the burden on neighboring registered entities, and assist in recovery of frequency. In addition, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. URE performed the required voltage analyses and found no conditions that required URE to establish different operating rules based on voltage. Finally, while URE's planning did not fully address performance requirements in the near-term and long-term planning horizons, URE addressed near-term and operational needs through other studies.

SERC2016015460 BAL-002-1 R4 - OVERVIEW

SERC determined that in two instances URE failed to recover its Area Control Error (ACE) within 15 minutes of the start of a Disturbance Control Standard (DCS) event.

The cause of the violation was an insufficient contingency reserve operating procedure and software system deficiencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to restore ACE to the required value within 15 minutes following two separate DCS events could result in prolonged operation at reduced frequency and reliance on neighboring registered entities to provide generation to balance the load. Nevertheless, URE restored ACE within five minutes of the required recovery period for each instance. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two minutes and five minutes, from 15 minutes after the start of the Reportable Disturbance through when URE returned its ACE to zero.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Ensured it carried additional contingency reserves for three months, as required by the BAL-002 Standard for failure to meet the Disturbance Control Standard (DCS) criteria 100% of the time;
2. Installed two patches to applicable software systems to (a) correct system user interface issues; and (b) correct an operational issue;
3. Revised its contingency reserve operating procedure to reflect changes necessary to prevent a recurrence of delayed response to a DCS event; and
4. Completed training on the contingency reserve operating procedure.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016016157 BAL-003-1.1 R2 - OVERVIEW

SERC determined that URE failed to implement a revised Frequency Bias Setting (FBS) according to the assigned schedule. URE stated that it was aware of the impending implementation and its staff awaited the ERO posting notification. URE also stated that it did not receive notification of the posting or the FBS by the required implementation date.

The cause of the violation was human performance and lack of awareness. URE did not update its FBS in accordance with the implementation plan because it was not aware of the location of the revised FBS settings.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to implement correct FBS may result in an inaccurate calculation of ACE and related Control Performance Standards (CPS). In the short term, it could result in a reduced response from URE during a frequency excursion. In the long term, it could result in URE failing meet its

interchange responsibilities. Nevertheless, URE would have responded to frequency deviations with a larger change in generation than it was required to provide. The larger contribution would tend to reduce the excursion, reduce the burden on adjacent entities, and assist in recovery of frequency. URE addressed any Inadvertent Exchange resulting from the incorrect Frequency Bias on an hourly basis throughout the period. The calculation of CPS is a monthly requirement. While the Frequency Bias error existed for more than one month, CPS is calculated on a monthly basis and URE took slightly longer than a month to implement the revised FBS, so its effect on the calculation of CPS was minimal. No frequency excursions during the period are attributable to the incorrect Frequency Bias. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately one month, from the day after URE was required to implement the revised FBS through when URE implemented the revised FBS.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Immediately adjusted the Frequency Bias Setting in the URE ACE calculation, after confirming the validation of the new Bias settings with the ERO;
2. Approved revisions to the operations process document to reflect changes in the BAL-003 Standard relating to the changing of the FBS;
3. Had all staff in the relevant department complete a read-and-sign of the updated version of URE's Frequency Bias Adjustment Procedure; and
4. Employed multiple calendar reminders leading up to and shortly after the annual requirement dates for updating the Frequency Bias to remind multiple URE staff of the need to change the setting in a timely fashion.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015526 FAC-014-2 R3 - OVERVIEW

SERC determined that URE failed to produce evidence that it performed voltage stability analyses when establishing SOLs as required by its SOL methodology.

The cause of this violation was URE's lack of a documented process and schedule, and insufficient training and internal controls to ensure that personnel performed and retained evidence of the voltage stability analyses required by URE's SOL methodology.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its SOL methodology to establish SOLs for at least three-and-a-half years could result in URE entering unsafe operational configurations that could damage equipment or cause system instability. Additional facts helped mitigate the risk of the violation. Although URE had not established SOLs based on voltage stability analyses, it performed contingency analyses that included voltage considerations. As a result, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. After discovering the violation, URE performed the required voltage analyses and found no conditions that required URE to establish SOLs based on voltage. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately three-and-a-half years, from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the TPL-001-4 study to identify any potential voltage issues starting in the summer of the following year and found none;
2. Approved its TPL-001-4 steady state procedure, which documents the steps necessary to analyze the non-converged contingencies that may identify potential voltage issues;
3. Developed its FAC-014-2 process document to assist staff in compiling the list of established SOLs/Interconnection Reliability Operating Limits (IROLs). Specifically, outlined the review process for non-converged contingencies identified in the TPL-001-4 Planning Assessment and the inclusion of the identified facilities in the SOL/IROL list;
4. Developed detailed project schedules documenting future requirements and due dates. Specifically, created tasks in project schedules to incorporate non-converged contingency analysis, compliance checkpoints, and the posting of SOL/IROLs;
5. Provided updated schedules and documentation to the appropriate subject matter experts for review and acknowledgement;
6. Provided training on solutions for non-converged contingencies to the appropriate subject matter experts;
7. Developed a TPL-001-4 stability process document covering any additional SOLs that resulted from the stability study; and
8. Provided updated TPL-001-4 stability process document for subject matter expert review and acknowledgement.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015527 FAC-014-2 R4 - OVERVIEW

SERC determined that URE failed to produce evidence that it performed voltage stability analyses when establishing SOLs as required by the Planning Authority's SOL Methodology.

The cause of this violation was URE's lack of a documented process and schedule and insufficient training and internal controls to ensure that personnel performed and retained evidence of the voltage stability analyses required by the Planning Authority's SOL methodology.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its Planning Authority's SOL methodology to establish SOLs for at least three-and-a-half years could result in URE entering unsafe operational configurations that could damage equipment or cause system instability. Additional facts helped mitigate the risk of the violation. Although URE had not established SOLs based on voltage instability, it performed contingency analyses that included voltage considerations. As a result, URE operators would have been aware of system configurations in which voltage stability would have been operationally limiting in the next-day and real-time operating horizons. After discovering the violation, URE performed the required voltage analyses and found no conditions that required URE to establish SOLs based on voltage. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately three-and-a-half years from the date the audit period began through when URE completed its Mitigation Plan.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the TPL-001-4 study to identify any potential voltage issues starting in the summer of the following year and found none;
2. Approved its TPL-001-4 steady state procedure, which documents the steps necessary to analyze the non-converged contingencies that may identify potential voltage issues;
3. Developed its FAC-014-2 process document to assist staff in compiling the list of established SOLs/ IROLs. Specifically, outlined the review process for non-converged contingencies identified in the TPL-001-4 Planning Assessment and the inclusion of the identified facilities in the SOL/IROL list;

4. Developed detailed project schedules documenting future requirements and due dates. Specifically, created tasks in project schedules to incorporate non-converged contingency analysis, compliance checkpoints, and the posting of SOL/IROLs;
5. Provided updated schedules and documentation to the appropriate subject matter experts for review and acknowledgement;
6. Provided training on solutions for non-converged contingencies to the appropriate subject matter experts;
7. Developed a TPL-001-4 stability process document covering any additional SOLs that resulted from the stability study; and
8. Provided updated TPL-001-4 stability process document for subject matter expert review and acknowledgement.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2017016808 PRC-002-2 R5; R5.3 - OVERVIEW

SERC determined that URE failed to notify one Transmission Owner, within 90 calendar days of completion of Part 5.1, that certain BES Elements required dynamic Disturbance recording (DDR) data.

The cause of this violation was insufficient procedures and training resulting in the human error in communicating incorrect information.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to notify a Transmission Owner that certain of its BES Elements required DDR data could result in insufficient data to analyze a disturbance on the BPS. Nevertheless, DDRs are used for forensic analyses following a disturbance and do not affect real-time operation or long-term or short-term planning of the BPS. While URE notified the Transmission Owner that certain of its BES Elements required DDR data approximately 40 days late, Transmission Owners have four years to reach 50% compliance and six years to reach full compliance with the installation requirements. This violation did not cause or prevent a disturbance, and the Transmission Owner did not receive a request for the DDR data to analyze a disturbance during this violation. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately 40 days, from the day after URE should have notified the Transmission Owner that DDR data was required through when URE notified the Transmission Owner that DDR data was required.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Notified the Transmission Owner in question that DDRs are necessary;
2. Updated its PRC-002-2 procedure to include an additional verification of the list of affected Transmission Owners;
3. Added tasks to the PRC-002-2 annual project plan to address this new step; and
4. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and procedure.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015697 PRC-023-3 R6 - OVERVIEW

SERC determined that URE failed to apply criterion B4 in Attachment B to the assessment it conducted in a single year. SERC later determined that URE also did not conduct an assessment within the prior calendar year, and thus did not apply any of the criteria in Attachment B in that calendar year. URE was not aware of the requirement to perform an assessment at least once each calendar year, but did perform its next assessment within 15 months of the prior assessment.

The cause of this violation was an inadequate process and deficient procedures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to identify low voltage transmission lines that may need to operate under temporary overload during contingencies may exacerbate those events. In this case, URE had performed the other required assessments in the second year and had informed the affected Transmission Owners of transmission lines requiring set point reviews. When URE completed the criterion B4 analyses, it determined that approximately 6% of the lines no longer met the criteria and 0.6% of the additional lines met the criteria requiring reviews. URE provided the revised list of circuits to all relevant parties within 30 days. The newly added transmission lines only met the B4 criterion under certain multiple contingency conditions. Since circuits identified through the criterion B4 analyses were related to the one-to-five year planning horizon, the delayed assessment did not result in an imminent risk to the BPS. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately five months from the date after the last date URE should have performed the assessment within the calendar year, through when URE completed the assessment that included the required criterion B4 analyses.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed its annual assessment including the B4 assessment, which is within the required calendar year, not to exceed a 15-month timeframe;
2. Added compliance checkpoints into the resource project schedules;
3. Updated the annual schedule with a log to capture milestone completion dates;
4. Created detailed annual and monthly checklists, including appropriate annual and monthly checkpoints according to PRC-023-3 R6;
5. Updated its PRC-023 process document, which includes references to the annual and monthly checklist; and
6. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and process documentation.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015532 TPL-002-0b R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not demonstrate that system performance met all Category B contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category B contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not demonstrate that system performance met all Category B contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE analyzed system

configurations similar to these Category B contingencies during contingency analyses, and would have identified problems in the short-term planning and operating horizon. URE's assessments did not demonstrate that system performance met Category B contingencies for a small number of Category B contingencies that typically do not present a large risk to the BPS. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;
5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015533 TPL-003-0b R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not demonstrate that system performance met all Category C contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category C contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not demonstrate that system performance met all Category C contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE addressed near-term and operational needs through other studies. URE assessments did not demonstrate that system performance met Category C contingencies for a relatively small number of Category C contingencies, which have a low probability of occurring. Consideration of system response to Category C contingencies is only part of the assessment process. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;

5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

SERC2016015534 TPL-004-0a R1; R1.3 - OVERVIEW

SERC determined that URE failed to complete the required assessments by resolving non-converged contingencies and thus did not show system performance following all Category D contingencies. While performing an internal compliance review, URE discovered that some assessments in two years resulted in non-converged contingencies.

Although URE shared the assessment results with its applicable Transmission Planners, URE could not demonstrate that it reviewed all non-converged contingencies in the two years of TPL assessments to determine the cause of the non-convergence and demonstrate that system performance met those contingencies. As a result, URE's assessments did not demonstrate that system performance met all Category D contingencies.

The cause of this violation was that URE did not have a process in place that addressed how staff should resolve such non-converged contingencies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not show system performance following all Category D contingencies, which could result in URE overlooking modifications and enhancements needed to meet performance requirements in the near-term and long-term planning horizons. Nevertheless, URE addressed near-term and operational needs through other studies. URE assessments did not show system performance following the relatively small number of Category D contingencies, which have a low probability of occurring. Consideration of system response to Category D contingencies is only part of the assessment process. No harm is known to have occurred.

SERC determined the duration of the violation to be approximately two years, from the date after URE should have completed a valid assessment through when URE documented the results of its non-converged contingency analysis in its next TPL-001-4 study.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. Completed the non-converged contingency analysis in the next TPL-001-4 study to identify any potential voltage issues, and found none;
2. Adjusted the TPL-001-4 steady state assessment project schedule by creating a task to incorporate non-converged contingency analysis, along with creating compliance checkpoints. URE also added compliance checkpoints to the TPL-001-4 stability assessment project schedule;
3. Approved its TPL-001-4 steady state procedure document, which documents the steps necessary in the TPL-001-4 annual steady state planning assessment to analyze the non-converged contingencies that may identify potential voltage issues;
4. Added tasks to the TPL-001-4 stability assessment project schedule to incorporate non-converged contingency analysis;
5. Completed training (read/sign documentation) for the appropriate subject matter experts for the updated schedule and documentation and completed training (read/sign documentation) for the appropriate subject matter experts on solutions for non-converged contingencies; and
6. Developed a TPL-001-4 stability process document and completed training (read/sign documentation) for the appropriate subject matter experts.

URE certified that it had completed all mitigation activities. SERC has verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of five hundred thousand dollars ($500,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. The instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE admitted to the violations and accepted responsibility for them;
3. URE agreed to the following changes to its organizational matrix and compliance culture:
    a. Reassigning the role of the CIP senior manager.
    b. Formation of a new group whose sole responsibility is the security of URE's Cyber Assets. This team performs URE's active CVA yearly.

c. Formation of a certain group whose responsibility is to oversee the quality of the work conducted by IT.

d. Reorganization of a relevant department such that it is no longer responsible for the security of URE's assets. It now concentrates its efforts on compliance matters and advising IT. The relevant department hired a new manager; this allowed the upper management of the department to focus on strategic matters rather than day-to-day operations.

e. Hired a CIP compliance subject matter expert with years of experience. This individual brought a different perspective to URE that has allowed it to enhance its compliance culture.

f. Shifted ownership of compliance responsibility from the compliance group to IT subject matter experts—removing the past practices of the compliance group being a buffer between subject matter experts and auditors.

g. Developed a program to encourage its employees to proactively identify and report potential violations of NERC Reliability Standards.

4. URE had an internal compliance program at the time of the violations, but SERC determined that, given the difficulties described above, the quality of URE's compliance program was deficient in demonstrating URE's compliance with the CIP standards and requirements. Therefore, SERC considered it to be a neutral factor;

5. URE's lack of cooperation and failure to timely submit its Mitigation Plans, failure to timely complete its Mitigation Plans, and failure to provide adequate evidence of completion of Mitigation Plans;

6. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

7. Although the risk posed to the BPS by the individual violations ranged from minimal to serious (26 minimal, 28 moderate, and 5 serious), the collective risk of the 59 violations posed a serious risk to the reliability of the BPS; and

8. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of five hundred thousand dollars ($500,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on August 8, 2017 and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of five hundred thousand dollars ($500,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Holly A. Hawkins* General Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 357-7914 – facsimile hhawkins@serc1.org Gary J. Taylor* President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8205 (704) 357-7914 – facsimile gtaylor@serc1.org	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Anne Faugust* Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Timothy E. Ponseti* Vice President, Operations SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8202 (704) 357-7914 – facsimile teponseti@serc1.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Leigh Anne Faugust
Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 31, 2017

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP18-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

NERC respectfully requests that the Commission accept this Spreadsheet NOP.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

	A	B	C	D	E	F	G	H
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**
2	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002165	Settlement Agreement	WECC_URE1 submitted a Self-Certification stating that it had a possible issue of noncompliance of CIP-006-1 R1. A WECC SME reviewed the supplemental data and conducted telephone interviews with WECC_URE1's compliance personnel. Based on the interviews with WECC_URE1, the WECC SME confirmed WECC_URE1 failed to create and maintain a Physical Security Plan, approved by a senior manager or delegate. Based on the investigation and available information, the SME determined WECC_URE1 was in possible violation of CIP-006-1 R1. The SME forwarded the findings to WECC Enforcement. WECC Enforcement reviewed the information submitted by WECC_URE1 and the SME's findings, and determined WECC_URE1 was in violation of CIP-006-1 R1, due to WECC_URE1's failure to create and maintain a Physical Security Plan, approved by a senior manager or delegate. Additionally, WECC_URE1 submitted a Self-Report for CIP-004-3 R4. In this instance, a security guard clicked the wrong checkbox in the physical access management system and gave the contractor in scope inadvertent access to a Physical Security Perimeter (PSP). When the security guard updated WECC_URE1's CIP-004-3 R4 access list, they realized and corrected the error. A WECC SME discussed the violation with WECC_URE1 and determined that the instance of noncompliance was actually a violation of CIP-006-3 R1.4, instead of a CIP-004-3 R4 violation. WECC added this instance of noncompliance to the scope of the above open enforcement action. The duration of this violation was approximately 81 months.	CIP-006-1	R1
3	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2014014941	Settlement Agreement	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-005-3a R1.5. Specifically, WECC_URE2 failed to test backup media to ensure information essential to recovery is available, as specified in CIP-009-3 R5, and required by CIP-005-3 R1.5 for Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter (ESP). This issue affected 12 Cyber Assets. The cause of this issue was a lack of proper settings and procedures for the affected routers and switches. The data to successfully recover the affected assets was stored on a server that had been decommissioned and whose data was stored in a format that was irretrievable. WECC determined that this violation began when a server was decommissioned and the data to successfully recover the affected assets was no longer readily available, and ended when WECC_URE2 implemented changes to its settings so that configurations are written to a remote server when the configuration is altered, and performed manual backups on firewalls to servers, which are themselves backed up, for a total of 1,371 days of noncompliance.	CIP-005-3a	R1
4	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2015014926	Settlement Agreement	WECC_URE2 submitted a Self-Report stating that it was in violation of CIP-006-3c R2.2. Specifically, WECC_URE2 failed to implement the protective measures specified in CIP-007-3 R5 and R6, needed to prevent unauthorized physical access to one Physical Security Perimeter (PSP). WECC_URE2 discovered that an employee, who was not authorized to grant access, was granting unauthorized personnel physical access to a PSP using other users' Physical Access Control System (PACS) credentials to make the change. WECC_URE2 investigated the incident and determined that the accounts were not properly managed and that the monitoring was insufficient to timely discover the unauthorized activity. The cause of this issue was that the field controllers were not identified as being a PACS elements so they were not captured under the CIP management functions. Staff turnover and unclear roles and responsibilities between the maintenance, physical security, and IT groups led to this misidentification. Additionally, there was insufficient monitoring to discover the unauthorized activity due to inadequate procedures. The PACS application audit log for users was available, but not reviewed until a problem was discovered via direct observation. WECC determined that this violation began when WECC_URE2 first failed to implement various protective measures, required by CIP-006 R2.2, and ended when WECC_URE2 completed its mitigating activities for a total of 1,400 days of noncompliance.	CIP-006-3c	R2

	I	J	K	L	M	N	O
1	**Violation Risk Factor**	**Violation Severity Level**	**Risk Assessment**	**Violation Start Date**	**Violation End Date**	**Total Penalty or Sanction ($)**	**Method of Discovery**
2	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE1 failed to create and maintain a Physical Security Plan to ensure that all Cyber Assets in an identified Electronic Security Perimeter (ESP) are also located within a PSP. Failing to create and maintain a Physical Security Plan could allow Cyber Assets within that PSP to go unprotected, unmonitored, or unchecked. This could allow unauthorized physical access to Critical Cyber Assets (CCAs) within that PSP, which could be used to affect the operation of the BPS. As compensating measures, WECC_URE1 had security in place several years prior to the beginning of this violation at all WECC_URE1 projects. All security plans included significant attention to securing the powerhouses. FurtherWECC_URE1 had standard operating procedures and processes that werecompliant with other regulations at the time of the violation. For these reasons, WECC determined that this violation posed a moderate risk to the reliability of the BPS.	When the Standard became mandatory and enforceable on WECC_URE1	When WECC_URE1 finished transitioning to CIP Version 5	No Penalty	Self-Certification
3	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, WECC_URE2 failed to provide evidence of testing back up media for network equipment. Failure to annually test backup media for Cyber Assets used in the access control and/or monitoring of the ESP could lead to recovery plans that are ineffective. Alternatively, WECC_URE2 may be forced to restore outdated information from a known good backup image in order to resume normal operations. However, WECC_URE2 had several controls in place to prevent and detect irrecoverable CCAs and their potential effect to the BPS. These controls include that there are redundant hardware and configurations in production and the Quality Assuranc environment, so the proper configuration could be taken from the Quality Assurance environment, and Cyber Vulnerability Assessments were performed annually on the configuration.	When the server was decommissioned and the data to successfully recover the affected assets was no longer readily available	When WECC_URE2 implemented changes to its settings so that configurations are written to a remote server when the configuration is altered, and performed manual backups on firewalls to servers, which are themselves backed up	No Penalty	Self-Report
4	Medium	Severe	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, WECC_URE2 control measures needed to prevent unauthorized physical access to a PSP. Failure to control access to restricted areas, such as a PSP, could result in unauthorized access by adversaries, who could ultimately gain access to protected BPS Cyber Assets. However, WECC_URE2 had several controls in place to prevent and detect the unauthorized access to the BES Cyber Assets, including, monitoring of the PSP; regular maintenance and testing of the field controllers; Personnel Risk Assessments were completed for all people involved in the incident; the PACS monitoring was functioning; WECC_URE2's access control process indicated the unauthorized access; PACS audit logs were functioning and upon review captured all unauthorized actions; appropriate patching was taking place for server/operating system and applications; and server/operating system user reviews were performed.	When WECC_URE2 first failed to implement various protective measures, required by CIP-006 R2.2	Mitigation Plan completion	No penalty	Self-Report

	P	Q	R	S	T
1	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	To mitigate this violation, WECC_URE1: 1) updated its Physical Security Plan to include: i. defined operational or procedural controls to restrict physical access; ii. utilization of multiple different physical access controls to collectively allow unescorted physical access into PSPs to only those individuals who have authorized unescorted physical access; iii. monitoring for unauthorized access through a physical access point into a PSP; iv. an alarm or alert in response to detected unauthorized access through a physical access point into a PSP to the personnel identified in the Bulk Electric System (BES) Cyber Security Incident response plan within 15 minutes of detection; v. monitoring of each Physical Access Control Systems (PACS) for unauthorized physical access; vi. an alarm or alert in response to detected unauthorized physical access to a PACS to the personnel identified in the BES Cyber Security Incident response plan within 15 minutes of the detection; vii. logged entries of each individual with authorized unescorted physical access into each PSP, with information to identify the individual and date and time of entry; viii. retaining of physical access logs of entry of individuals with authorized unescorted physical access into each PSP for at least 90 calendar days; and ix. restricted physical access to nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter (ESP) in those instances when such nonprogrammable communication components are located outside of a PSP; 2) implemented extensive modifications to the existing security systems at all of its Critical Assets; 3) updated the current Physical Security Plandocumentation or created documents, where only informal procedures were in place; and 4) procured and developed a PACS test bench to evaluate new software and hardware and to test new components to the system.	7/1/2016	10/7/2016	Does Not Contest	WECC considered WECC_URE1's compliance history and determined there were no relevant instances of noncompliance.
3	To mitigate this violation, WECC_URE2: 1) implemented anarchive command on switches and routers, so configurations are written to a remote server when the configuration is altered, and performed manual backups on firewalls to server, which are themselves backed up; 2) ensured backup/configuration/compliance information is stored in a generic format that can be recovered without special software; and 3) revised backup processes to ensure backups are done consistently, so media testing can take place.	6/9/2016	12/15/2016	Does Not Contest	WECC did not give credit for WECC_URE2's Internal Compliance Program (ICP). Although WECC_URE2 does have a documented ICP that has been provided to WECC, WECC determined that, due to the length of the violation, WECC_URE2's ICP failed, in this instance, to adequately detect the violation in a timely manner.
4	To mitigate this violation, WECC_URE2: 1) either deleted the non-approved access or provided approval for access, depending on need; 2) implemented proper user account controls, according to CIP version 5; 3) clarified and documented roles and responsibilities for all parts of PACS management, including ensuring PACS roles and responsibilities were clear and communicated; 4) ensured user account controls are addressed in CIP version 5 transition; and 5) completed an administrative action for the employee who improperly granted access.	7/1/2016	12/9/2016	Does Not Contest	WECC did not give credit for WECC_URE2's Internal Compliance Program (ICP). Although WECC_URE2 does have a documented ICP that has been provided to WECC, WECC determined that, due to the length of the violation, WECC_URE2's ICP failed, in this instance, to adequately detect the violation in a timely manner.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

February 28, 2018

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP18-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of two violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2017). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two million seven hundred thousand dollars ($2,700,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	**Standard**	**Req.**	**VRF/VSL**	**Discovery Method***	**Risk**	**Penalty Amount**
WECC2016016233	CIP-003-3	R4	Medium/ Severe	SR	Serious	$2.7M
WECC2016016234	CIP-003-3	R5	Lower/ Severe			

Background to the Violations

URE received a report of an online data exposure with data possibly associated with URE. The report came from a white hat security researcher not associated with URE. A third-party URE contractor exceeded its authorized access by improperly copying certain URE data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. The contractor failed to comply with URE's information protection program on which it was trained. While the data was on the contractor's network, a subset of live URE data was accessible online without the need to enter a user ID or password. This subset of data included over

30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names.

The information associated with the CCAs was accessible on the Internet for a total of 70 days. URE also reviewed the system logs of the contractor and found that the logs showed unauthorized access to the URE data subset from unknown IP addresses, as well as IP addresses associated with the white hat security researcher who notified URE of the data exposure.

URE informally notified WECC of the incident and explained how URE was managing the situation. URE and WECC had multiple discussions and meetings about the situation over the next two months. Four months after it had discovered the incident, URE submitted an incident update to WECC.

Based on information from URE's incident report and WECC data requests, WECC recommended URE file Self-Reports for the issues. WECC determined URE failed to implement adequately its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. WECC also determined URE failed to implement adequately a program for managing access to protected information related to CCAs, as required by CIP-003-3 R5.

Analysis of the system logs showed that only the security researcher executed commands to view and download data. More detailed system logs would be required to determine definitively that no other third party had downloaded the data, but the short duration of the connections decreased the likelihood that additional accessing or downloading of data had occurred. To recover the exposed data, URE contacted the security researcher and requested that he securely return the data, securely delete all copies of the data from his system, and submit to URE a signed, notarized affidavit confirming that he deleted all copies of the data.

RISK COMMON TO THE VIOLATIONS

These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs associated with the data exposure include servers that store user data, systems that control access within URE’s control centers and substations, and a supervisory control and data acquisition (SCADA) system that stores critical CCA Information. The data was exposed publicly on the Internet for 70 days. The usernames of the database were also exposed, which included cryptographic information of those usernames and passwords.

Exposure of the username and cryptographic information could aid a malicious attacker in using this information to decode the passwords. This exposed information increases the risk of a malicious attacker gaining both physical and remote access to URE's systems. A malicious attacker could use this

information to breach the secure infrastructure and access the internal CCAs by jumping from host to host within the network. Once in the network, the attacker could attempt to login to CCAs, aided by the possession of username and password information.

WECC found URE had implemented limited compensating controls to reduce the risk associated with a malicious actor gaining access to its system during the noncompliance. URE did not classify the data as CIP-protected information because it was on a pre-production server, nor were there any controls in place to prevent the contractor from taking the data off premises and putting it on their own Internet-facing network. URE had implemented simple-character usernames similar to the usernames that were publicly exposed. In addition, URE did not implement any preventive or detective controls. URE only discovered the data exposure because of an external white hat security researcher who found the publicly accessible data on the Internet.

URE has three firewalls between the external network and the assets inside the Electronic Security Perimeter that make it difficult for a malicious actor to access URE's CCAs. Based on the controls WECC analyzed, there was lower probability that this instance of noncompliance would have caused an impact to the reliability of the BPS at the time of its occurrence. Nevertheless, there is no reasonable assurance that during the time the data was exposed on the Internet, it was not already used by a malicious actor – or collected by such an actor – to access URE's network and install an application that can cause the potential harm in the future. The additional sanction described below is intended to address this residual risk.

MITIGATION ACTIVITY COMMON TO THE VIOLATIONS

URE submitted identical Mitigation Plans to address the referenced violations. To mitigate these violations, URE:

1. Required the vendor to shut down their software development server, thereby ending the data exposure;
2. Performed three different forensic analyses to verify that only the security researcher accessed the data during the time of the exposure;
3. Required the security researcher to provide the data to the IT department, delete the data from his computer, and attest in an affidavit that these items were complete;
4. Removed vendor access to the asset management database in the datacenter. To allow vendors to perform development work on projects, URE implemented a process whereby an authorized URE employee must copy the source code from the asset management database and securely transfer it to the software development vendor. Upon work

completion, the vendor would then securely transfer the new version of code to an authorized URE employee who would load it back onto the asset management database;

5. Changed access controls to the database. URE also deployed a suite program to provide policies and controls to prevent confidential-Bulk Electric System (BES) Cyber System Information or restricted-BES Cyber System Information classified emails and attachments from being sent to outside email addresses;
6. Improved security controls for vendor management by requiring vendors to take information security and privacy awareness training annually, implementing a new vendor remote access platform, and enhancing policies, background checks, and contract language for vendor employees; and
7. Classified all BES Cyber System Information for both production and non-production assets.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

VIOLATION DESCRIPTIONS

CIP-003-3 R4 - OVERVIEW

WECC determined that URE did not adequately implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. Specifically, in the above described incident, WECC found that URE failed to adequately implement the following areas of its program to identify, classify, and protect information associated with CCAs:

1. URE failed to identify and classify the information used in the system in accordance with its information protection policy. URE stated it did not classify in accordance with its policy because the information was part of a pre-production asset management system. Even though the data was in a pre-production system, it is live CCA Information, and URE was required to implement a program to identify, classify, and protect this information.
2. Due to URE's failure to classify the information, URE also failed to provide the proper protections during storage and transmission, distribution, and duplication, in accordance with its policy.
3. URE failed to designate the system and the contractor's network IP as a CCA Information approved storage location and store CCA Information in an approved location.
4. URE failed to ensure that personnel handling CCA Information adhered to URE's protection measures.

5. URE failed to activate its existing policies or procedures for sharing protected information with third parties before information was disseminated, either electronically or physically, in accordance with its policy.

The cause of this violation was URE's failure to apply its information protection program to the CCA Information in its pre-production environment.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 590 days, from the date the third-party contractor exposed the information on the Internet, through when URE completed classifying all CCA Information for production and non-production assets. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

CIP-003-3 R5 - OVERVIEW

WECC determined that URE did not implement a program for managing access to protected CCA Information, as required by CIP-003-3 R5. Specifically, in the above described incident, WECC found that URE failed to ensure that the contractor protected the CCA Information when it improperly copied the data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. In response to a data request, due to the fact that the contractor copied the data to an unapproved location, URE stated that the security controls for the contractor's storage location were not understood or documented. WECC found that URE did not understand or document the security controls at the contractor's location before it released information to the contractor, and afterward, when the data was exposed to the Internet, it failed to adequately implement its program for managing access.

The cause of this violation was URE's failure to ensure its contractor followed its information protection program and procedures on which the contractor was trained.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 80 days, from the date the third-party contractor exposed the information on the Internet, through when the white hat security researcher deleted all remaining electronic copies of data and screen shots from his hard drive and sanitized his device to prevent future access. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two million seven hundred thousand dollars ($2,700,000) for the referenced violations as well as a non-monetary sanction. As an additional sanction designed to reduce the opportunities for a malicious actor to use the exposed data, WECC required URE to set its relevant CIP passwords-remembered to "all" or the maximum the system will remember to prevent passwords from being used more than once, or to maximize the frequency for which a password may be used.

In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE had an internal compliance program at the time of the violation;
3. URE self-reported the violations;
4. URE was not fully transparent and forthcoming with all pertinent information detailing the data exposed in the incident. Specifically, URE did not provide WECC initially with all the data fields exposed in the incident;
5. the violations posed a serious and substantial risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two million seven hundred thousand dollars ($2,700,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on February 6, 2018, and approved the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two million seven hundred thousand dollars ($2,700,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz Heather Laws* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz	Sonia C. Mendonça* Vice President, Acting General Counsel and Corporate Secretary, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Leigh Anne Faugust* Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Leigh Anne Faugust

Sonia C. Mendonça
Vice President, Acting General Counsel and Corporate Secretary, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Leigh Anne Faugust
Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 31, 2018

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity
FERC Docket No. NP18-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because ReliabilityFirst Corporation (ReliabilityFirst) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from ReliabilityFirst's determination and findings of 22 violations of the Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2018). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE admits to the violations and has agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between ReliabilityFirst and URE. The details of the findings and basis for the penalty are set forth herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2018), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth herein.

Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	**Standard**	**Req.**	**VRF/ VSL**	**Discovery Method* Date**	**Risk**	**Penalty Amount**
RFC2015014936	CIP-003-3	R5	Lower/ Severe	SR	Minimal	$180K
RFC2016015692	CIP-003-3	R5	Lower/ Severe	SR	Moderate	
RFC2015015313	CIP-003-3	R6	Medium/ Severe	SR	Minimal	
RFC2016015717	CIP-003-3	R6	Lower/ Severe	SR	Minimal	
RFC2015015008	CIP-004-3a	R3	Medium/ Moderate	SR	Minimal	
RFC2015015009	CIP-004-3a	R4	Lower/ High	SR	Minimal	
RFC2015015402	CIP-004-3a	R4	Lower/ Severe	SR	Minimal	
RFC2016015716	CIP-004-3a	R4	Lower/ Severe	SR	Minimal	
RFC2016016474	CIP-005-3a	R1	Medium/ Severe	SR	Moderate	
RFC2015015314	CIP-006-3c	R1	Medium/ Severe	SR	Minimal	
RFC2016015844	CIP-006-3c	R5	Medium/ Severe	SR	Serious	
RFC2016015715	CIP-007-3a	R1	Medium/ Severe	SR	Minimal	
RFC2016015714	CIP-007-3a	R2	Medium/ Severe	SR	Moderate	

RFC2015015241	CIP-007-3a	R3	Lower/ Severe	SR	Minimal	
RFC2016015843	CIP-007-3a	R3	Lower/ Severe	SR	Minimal	
RFC2016015538	CIP-007-3a	R5	Lower/ Severe	SR	Minimal	
RFC2016015713	CIP-007-3a	R5	Medium/ Severe	SR	Moderate	
RFC2016015752	CIP-007-3a	R6	Medium/ Severe	SR	Moderate	$180K
RFC2015015107	CIP-007-3a	R6	Lower/ Severe	SR	Minimal	
RFC2017017565	CIP-007-6	R2	High/ Severe	CA	Minimal	
RFC2017017566	CIP-007-6	R5	Medium/ High	CA	Minimal	
RFC2015015312	CIP-014-2	R1	High/ Lower	SR	Moderate	

RISK COMMON TO THE VIOLATIONS

ReliabilityFirst determined the penalty in this case based on the six moderate risk violations and the one serious risk violation.

Fifteen of the violations posed a minimal risk, six posed a moderate risk, and one posed a serious and substantial risk to the reliability of the bulk power system (BPS). ReliabilityFirst determined the violations do not involve and are not indicative of programmatic issues across URE's CIP compliance program. URE implemented internal controls that identified many of the instant violations. While most of the violations were short in duration, or relatively short, several of the moderate risk violations had longer durations (up to two years), indicating a potential weakness in detective controls in these areas.

Nevertheless, these moderate risk violations generally involved isolated systems or assets, and thus, did not involve programmatic or systemic issues.

URE had some internal controls in place that mitigated the risk to the BPS. For example, URE's buildings and Physical Security Perimeters (PSPs) were under surveillance 24 hours a day, seven days a week; Physical Access Control Systems (PACSs) were isolated, requiring authorized physical and electronic access; Bulk Electric System (BES) Cyber Assets had both logical and physical protection; and URE used detective logging and alarming tools.

The serious risk violation provided the opportunity for undetected compromise of an unmanned, critical substation and showed URE's inability to respond due to lack of situational awareness. While the risk was somewhat mitigated because certain assets were being monitored via an alert and monitoring program, which would have detected unauthorized changes, and local physical access controls were working, URE's headquarters could not monitor or communicate with the site and thus would have been unaware of and unable to respond to an intrusion.

CIP-003-3 R5 (RFC2015014936) - OVERVIEW

ReliabilityFirst determined that URE failed to document and implement a program for managing access to protected Critical Cyber Assets (CCAs) as required by CIP-003-3 R5, in three separate instances. In two instances, employees did not immediately pick up printed versions of CIP documents from printers. In the third instance, URE inadvertently set the confidentiality classification level for a CIP process document to "public" view on its internal site.

ReliabilityFirst determined the duration of the violation to be approximately one year and nine months, from when the confidential document was inadvertently set to "public" view, to the date by which all three instances were mitigated by protecting or destroying the confidential information.

The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's contractor failed to protect CIP information as required. Workforce management was involved because, in all three instances, additional training and awareness could have helped to prevent these errors.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Identify and implement a technological solution to control and monitor end-point printing;
2. Train on and validate the solution's effectiveness;
3. Identify changes required to maintain integrity of documents within the document repository when updating, changing, or moving documents;
4. Prevent URE resources from uploading documentation directly to internal site through a certain mode, therefore forcing documentation to be added in an approved and documented method; and
5. Validate the metadata prior to document publication.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R5 (RFC2016015692) – OVERVIEW

ReliabilityFirst determined that URE failed to document and implement a program for managing access to protected CCAs as required by CIP-003-3 R5. Specifically, a URE reliability assurance team member was able to access a file in a URE NERC compliance information folder, which contained CIP protected information.

ReliabilityFirst determined the duration of the violation to be approximately two years and one month, from the date URE permitted unauthorized individuals access to CIP information, to the date URE completed its Mitigation Plan.

The violation involved the management practice of asset and configuration management because URE did not have an accurate understanding of the effects of the configurations of folders within its access system.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Investigate and resolve issues with folder permissions on the relevant folder;
2. Identify folders that contain information utilizing a certain document (URE's list of approved BES Cyber System information repositories) as well as existing enterprise job roles;
3. Contact CIP data owners to confirm that all of their repositories are listed on the relevant repository list document;
4. Create a procedure for how new file share repositories will be created on servers;
5. Create a procedure to migrate the folders identified in milestone two;

6. Migrate the relevant folders; and
7. Remove creator owner permissions from all shared folders identified in milestone two.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R6 (RFC2015015313) – OVERVIEW

ReliabilityFirst determined that URE failed to have minimum security management controls in place to protect CCAs. Specifically, an analyst added a device to URE's logging tool, and added the correct group to receive the alerting for the device. The next day, another analyst deleted the device from the logging tool. Thereafter, the logging tool was retaining logs for a certain device, but the device was not in the correct group to alert on the required conditions.

ReliabilityFirst determined the duration of the violation to be approximately four-and-a-half months, from the date the device was deleted and thus not alerting, to the date URE added the device to the correct alerting group.

The root cause of this violation was that an analyst did not follow the proper change management process despite being trained on the proper procedure for change management. This violation involved the management practices of asset and configuration management and workforce management. Asset and configuration management was involved because URE did not adhere to its configuration management process. Workforce management was involved because URE staff did not adhere to their internal procedures and controls in configuring a Cyber Asset.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Terminate the analyst as a result of not satisfactorily performing his job responsibilities relating to this incident and other actions;
2. Determine the extent of condition by verifying that all assets which are defined in URE's CCA lists are sending logs to the logging tool and are associated with the correct groups to generate alerts defined in a relevant security status monitoring process;
3. Evaluate the solution to monitor the configuration of the logging tool's log sources that controls CIP alerting and test email alerting;

4. Build a new rule in the logging tool to alert the manager of the cyber security department and the director of networks and information security department after the logging tool has not received logs from a certain period of time;
5. Implement a solution to monitor the logging tool's log source group defined that controls CIP alerting and configured email alerts to the cyber security team when there are changes to that group;
6. Update the processes and work forms associated with change management and commissioning to include specific controls an asset administrator must act upon to ensure CIP-005 and CIP-007 controls are addressed in alignment with the current CIP version; and
7. Conduct a page-turn training session of newly proposed processes and work forms, and address all applicable questions and concerns during the page-turn exercise.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-003-3 R6 (RFC2016015717) – OVERVIEW

ReliabilityFirst determined that URE failed to have minimum security management controls in place to protect CCAs. Specifically, in two instances URE did not follow the established change management process: first, when URE deployed a PACS intelligent controller into production, and second, when URE made changes to several assets.

ReliabilityFirst determined the duration of the violation to be approximately 10 months, from the date URE was required to comply with CIP-003-3 R6, to the date URE completed its Mitigation Plan.

Regarding the first instance, the root cause was lack of managerial oversight during a transition process where URE was transitioning the responsibility of the PACS devices from its security department, which did not have the appropriate technical expertise, to its engineering group. This violation occurred during the transition time when these Cyber Assets were being incorporated into the engineering group's change control process. Regarding the second instance, the violation involved the management practices of asset and configuration management and workforce management. Asset and configuration management was involved because URE did not adhere to its configuration management process. Workforce management was involved because URE staff did not adhere to their internal procedures and controls in configuring a Cyber Asset.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete changes to the engineering change control process to align with CIP Version 5;
2. Update engineering CIP Cyber Asset management system (CAMS) to align with the new change control process;
3. Develop CIP Version 5 capable baseline configuration in CAMS;
4. File and obtain approval of Technical Feasibility Exceptions (TFEs) for the PACS to complete CIP Version 5 commissioning tasks in CAMS;
5. Develop a separate security configuration procedure for the relevant controller;
6. Complete commissioning and change control tasks for assets installed at the relevant locations;
7. Establish a change review board;
8. Train all engineering personnel responsible for the use of CAMS for all CIP changes on related systems;
9. Implement a new change management tool; and
10. Train relevant teams on the use of the new change management tool.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R3 (RFC2015015008) – OVERVIEW

ReliabilityFirst determined that URE failed to have a documented Personnel Risk Assessment (PRA) program for personnel having authorized cyber or authorized unescorted physical access to CCAs. Specifically, URE granted four employees unescorted physical access without appropriately documented PRAs.

ReliabilityFirst determined the duration of the violation to be approximately one month, from the date URE granted unescorted physical access without the requisite PRAs, to the date URE revoked the access.

Regarding the root cause, a specialist reviewed a large number of identities over a three-day period during the rollout of URE's new role-based access process, which led to these four errors in the process. This violation involved the management practice of work management and verification as the errors were caused because of having to review many PRAs in a short period, and not conducting a review to verify that there were no errors in that review process.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Conduct individual counseling with the security specialist;
2. Conduct a meeting with the impacted groups to discuss the incident;
3. Conduct reinforcement training of all corporate security personnel involved with CIP-004-3 R3 compliance;
4. Formulate a likelihood risk-based PRA review methodology;
5. Conduct a review of PRA documentation for those identified individuals and took immediate action on any issues identified therein; and
6. Revise URE policy requiring URE corporate security to perform PRAs on all individuals requiring any level of unescorted access, whether CIP or non-CIP in nature, thus eliminating the reliance on another entity to perform the PRA.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2015015009) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, this violation involves three instances of URE not properly revoking access within the seven-day period.

ReliabilityFirst determined the duration of the violation to be approximately one year, from the date URE was required to comply with CIP-004-3a R4, to the date URE completed its Mitigation Plan.

The violation involved the management practice of workforce management because they involve employees taking some, but not all steps necessary to complete revocation in a timely manner as a result of rushing through the tasks. Additionally, URE could have had additional controls in place to ensure the employees completed all necessary steps to revoke access in a timely manner.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Modify the workflows for all access revocation-related requests to include a reviewer step;
2. Identify any additional identities with “invalid” termination dates;
3. Disable future termination capability;
4. Train system administrators of the identity access system regarding the capability changes and process handling;

5. Modify workflows to accommodate an escalation process for all individual access revocations; and
6. Review and revise the process and requirements for revocation of access when a temporary leave of absence occurs.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2015015402) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, access for one URE employee located at another registered entity's facility was not properly revoked within the seven-day period.

ReliabilityFirst determined the duration of the violation to be approximately four-and-a-half months, from the date URE was required to remove the employee's access to the date URE removed the access.

The root cause was that the registered entity that owned the facility the employee was located failed to follow the procedure for notifying URE when an employee no longer needs access. Additionally, URE's additional proactive measure, where URE sent weekly emails to the registered entity identifying the individuals who currently had access, failed because the registered entity did not properly review the weekly email. URE had been sending the registered entity the weekly emails since before the violation began. The email should have prompted the registered entity to inform URE of the individual's departure from the company within the required timeframe. The violation also involved the management practice of external interdependencies because URE failed to mitigate risks relating to third parties

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Request access removal form from the registered entity;
2. Receive access removal form;
3. Request follow-up resignation data regarding the employee in question;
4. Receive resignation data from the registered entity;
5. Receive results of the registered entity's internal investigation;
6. Set up a meeting with the registered entity to identify corrective or preventive actions;

7. Reinforce with the registered entity the CIP-004-3 and future CIP-004-5 access removal requirements;
8. Receive evidence of the registered entity's internal training regarding CIP-004 access removal requirements; and
9. Revise the unescorted physical access agreement between URE and the registered entity.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-004-3a R4 (RFC2016015716) – OVERVIEW

ReliabilityFirst determined that URE failed to maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs. Specifically, access for one URE employee was not properly revoked within the seven-day period after changing job duties within URE.

ReliabilityFirst determined the duration of the violation to be approximately two weeks, from the date URE should have removed access, to the date URE removed access.

The root cause was an unclear designation of CIP versus non-CIP access within URE's alert tool, which contributed to human performance issues in completing the access removal tasks. This violation involved the management practice of workforce management because additional training, along with clearer designations in the system, could have helped prevent this violation.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Introduce and train affected personnel on the new CIP Standards;
2. Launch a new CIP access revocation process; and
3. Email notifications from the alert tool with priority status to revoke CIP access initiated.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-005-3a R1 (RFC2016016474) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that every CCA resided within an Electronic Security Perimeter (ESP). Specifically, URE did not identify and document an access point to the ESP.

ReliabilityFirst determined the duration of the violation to be approximately one year and seven months, from the first date that a substation technician was dispatched to perform maintenance that required connection to both CAMs and a BES Cyber Asset, to the date URE completed its Mitigation Plan.

The violation involved the management practice of verification because URE failed to verify that it properly identified and understood all external routable connections and access points.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Update URE's cyber security policy to address that URE resources shall only utilize URE authorized Transient Cyber Assets (TCAs) when connecting to a High or Medium impact BES Cyber System(s), Protected Cyber Asset(s), and/or ESP(s);
2. Implement a project plan for TCAs that will include technical, procedural, and process controls to prevent TCA laptops from becoming unintended access points;
3. Drafted, as part of the project plan, a test plan which establishes technical controls that disable a TCA laptop's logical input and output ports (Ethernet and console ports) when connected to URE's Virtual Private Network (VPN);
4. Execute, as part of the project plan, the technical controls test plan and provide evidence showing the results that the TCA laptop's logical input and output ports are disabled when connected to URE's VPN.
5. Perform, as part of the project plan, training with URE resources in the field on how to use the technical and cyber security controls on a TCA laptop; and
6. Deploy, as part of the project plan, TCA laptops to authorized TCA users.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-006-3c R1 (RFC2015015314) – OVERVIEW

ReliabilityFirst determined that URE failed to document, implement, and maintain a physical security plan as required by CIP-006-3c R1. Specifically, during a routine inspection URE discovered that an air conditioning unit was an exploitable access point into an identified PSP.

ReliabilityFirst determined the duration of the violation to be approximately 11 months, from the date URE was required to comply with CIP-006-3c R1.1, to the date URE completed its Mitigation Plan.

The root cause was a lack of communication prior to installing the air conditioning unit. This violation involved the management practice of grid maintenance because URE failed to maintain properly its facilities.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Review the violation with the facilities manager to clearly identify the issue and impacts;
2. Seal and secure the access point to the PSP;
3. Conduct a lessons learned meeting to review the violation and the root cause with the supply chain and facilities group;
4. Create and publish a new process document; and
5. Conduct training of all affected groups on the process document.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-006-3c R5 (RFC2016015844) – OVERVIEW

ReliabilityFirst determined that URE failed to document and implement the technical and procedural controls for monitoring physical access at all access points to the PSPs 24 hours a day, seven days a week. Specifically, the power supply to a security rack was shut off during maintenance work at one of URE's facilities, and for six days afterwards the facility was not communicating with URE's headquarters.

ReliabilityFirst determined the duration of the violation to be approximately six days, from the date URE failed to monitor physical access, to the date URE restored monitoring capabilities.

The violation involved the management practices of grid maintenance and workforce management. Grid maintenance was involved because URE did not properly mitigate the risks of the maintenance work on the station. More specifically, URE's vendor properly submitted a maintenance ticket, but there was a miscommunication between groups, so URE and the vendor did not consider the security systems that operate on the same network where the maintenance activities were being performed.

ReliabilityFirst determined that this violation posed a serious and substantial risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete repairs and re-establish security monitoring at the relevant facility;
2. Conduct PACS incident lessons learned meeting;
3. Revise security command center alarm response policy to clarify responsibilities;
4. Review current processes and practices to determine a need for alignment with roles and responsibilities;
5. Revise or create documentation regarding roles and responsibilities;
6. Provide training on new or revised policies and processes regarding PACS outage reporting, troubleshooting, and communications;
7. Develop PACS service level agreement policy document that documents responsibilities for the use, maintenance, and management of physical security controls; and
8. Approve and implement PACS service level agreement.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R1 (RFC2016015715) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. Specifically, a URE asset administrator performed a PACS modification, but did not complete the change and configuration management process documentation for a device that was replaced.

ReliabilityFirst determined the duration of the violation to be approximately seven months, from the date URE introduced the assets into its environment, to the date by which URE completed the change control activities.

The root cause was a lack of workforce management in that the corporate security department charged with managing the assets did not have expertise to provide technical oversight of the PACS devices.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Complete changes to engineering change control process to align with CIP Version 5;

2. Update the engineering CIP CAMS to align with the new change control process;
3. Develop CIP Version 5 baseline configuration in the engineering CAMS.
4. File and obtain approval of TFEs for the PACS to complete CIP Version 5 commissioning tasks in CAMS;
5. Develop and implement a separate security configuration procedure for relevant controllers;
6. Complete commissioning and change control tasks for assets installed at the relevant locations; and
7. Train all engineering personnel responsible for the use of CAMS for all CIP changes on related systems.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R2 (RFC2016015714) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled. Specifically, URE had multiple undocumented services with ports enabled related to its PACS, and one of those ports was unnecessary for operations.

ReliabilityFirst determined the duration of the violation to be approximately eight months, from the date URE was required to comply with CIP-007-3a R2, to the date URE completed its Mitigation Plan.

The violation involved the management practices of verification and workforce management. Verification management was involved because URE failed to verify and document that the ports and services were necessary for operations.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Reassign these Cyber Assets to an asset manager capable of reviewing CIP controls;
2. Implement a new monitoring program; and
3. Verify its Cyber Vulnerability Assessment (CVA) Action Plan to remove the undocumented ports and accounts.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-6 R2 (RFC2017017565) – OVERVIEW

ReliabilityFirst determined that URE failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R2-Security Patch Management. Specifically, URE was two weeks late in completing evaluations of security patches for two Cyber Assets, which were both PACS.

ReliabilityFirst determined the duration of the violation to be approximately two weeks, from the date by which URE was required to complete the evaluations, to the date URE completed the evaluations.

The root cause was an error in calculating the date to perform the evaluation of security patches. The calculation for the next security patch evaluation was based on the implementation of the previous month's security patches rather than the previous evaluations.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Conduct a meeting to discuss patch evaluation process changes with asset managers;
2. Draft proposed document changes and distribute them for comments;
3. Hold a meeting to review and finalize changes to process documents with asset managers;
4. Publish updated documents to URE's internal site; and
5. Determine if automatic notifications can be implemented based on available technology and resources.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R3 (RFC2015015241) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP. Specifically, URE failed to install three sets of patches in a timely manner, and no compensating measures were documented to mitigate risk exposure.

ReliabilityFirst determined the duration of the violation to be approximately three-and-a-half months, from the date by which URE was required to implement the first set of patches, to the date URE evaluated the third set of patches.

The root cause is that there were too many individuals involved in the patching process and roles and responsibilities were not clear. Additionally, this violation involved the management practice of asset and configuration management because URE's processes lacked sufficient controls to manage the timely implementation of changes to assets.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Facilitate CIP server patching transition meetings;
2. Have the engineering department walk through the current process with the server team;
3. Take an inventory and review CIP forms by asset type/class that are completed by the engineering and security departments for CIP patching with the server team;
4. Implement a relevant patching tool and integrate it to all applicable CIP Cyber Assets;
5. Provide the server team with asset baseline information and historical patching data;
6. Have the engineering department provide a review of the previous patch evaluation performed by the server team;
7. Transition the operating system patch management duties for certain servers to the server team;
8. Update process documents to reflect common process across the multiple asset classes the server team will be handling in the future;
9. Perform an extent of condition assessment to identify any missing patches on the Cyber Assets; and
10. Remediate all missing patches on all applicable CIP Cyber Assets following the change management process.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R3 (RFC2016015843) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, document, and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP. Specifically, URE failed to patch a certain server and failed to evaluate software supplied and installed by URE on associated devices.

ReliabilityFirst determined the duration of the violation to be approximately one year and eight months, from the date the asset was declared a PACS, to the date URE completed its Mitigation Plan.

The root cause was miscommunication between URE and its vendor. The vendor agreement stated that the vendor would assist in the evaluation and implementation of patches. The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's coordination with the external vendor did not assure that patches were installed in a timely fashion. Workforce management was involved because URE staff did not properly secure or control the PACS logging system.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Patch the relevant server;
2. Update procedures to include the relevant server in the server teams' procedure;
3. Incorporate the relevant server into the server team's monthly patching process;
4. Perform an extent of condition assessment to find and address any other CIP assets that have any patching deficiencies; and
5. Remedy any patching deficiencies found during the extent of condition assessment.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R5 (RFC2016015538) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Specifically, URE did not change one password for a relay despite documentation stating the password was changed.

ReliabilityFirst determined the duration of the violation to be approximately three months, from 15 months from the prior password change, to the date URE changed the password.

This violation involved the management practice of verification, as URE did not have a verification process to ensure that all passwords were changed.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Update the relevant driver to support a relevant relay model, which allows for the automatic update of passwords to occur annually;
2. Revise the relevant baseline testing and approval of engineering Cyber Assets process to include a step/instruction to update the relevant drivers if applicable; and
3. Train employees and contractors during a safety stand down.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R5 (RFC2016015713) – OVERVIEW

ReliabilityFirst determined that URE failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access. Specifically, URE had three relevant instances wherein user accounts were either not documented, had insufficient administrator rights, or lacked approved access records.

ReliabilityFirst determined the duration of the violation to be approximately one year and seven months, from the date URE was required to comply with CIP-007-3a R5, to the date URE completed its Mitigation Plan.

The violation involved the management practices of external interdependencies and workforce management. External interdependencies management was involved because URE's access provision for its external vendor did not provide the necessary approval. Workforce management was involved because URE staff did follow procedures to document user accounts properly.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Reassign the relevant Cyber Assets to an asset manager capable of reviewing CIP controls;
2. Implement a new baseline monitoring program;
3. Verify that its CVA Action Plan to remove the undocumented accounts was implemented;
4. Establish a team and conduct a series of meetings to develop a service level agreement between departments;
5. Use the service level agreement forum to determine the required permissions for each functional group;
6. Implement the appropriate access between each functional group;

7. Include relevant security shared accounts in an URE centralized password safe;
8. Create relevant security roles in the access request system to document who has access to the password safe; and
9. Create requests and grant access through the access request system for individuals needing access to the relevant security system.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-6 R5 (RFC2017017566) – OVERVIEW

ReliabilityFirst determined that URE failed to implement one or more documented processes that collectively include each of the applicable requirement parts in CIP-007-6 Table R5-System Access Controls. Specifically, URE failed to change passwords at least once every 15 calendar months for a shared account that could be used for interactive user access for two Cyber Assets, both PACS.

ReliabilityFirst determined the duration of the violation to be approximately two-and-a-half months, from the date by which URE should have changed the passwords, to the date by which URE changed the passwords.

The root cause was an error during transition when the servers came under the ownership of the server team. The violation involved the management practice of verification because URE failed to verify that each PACS had current patches after the transition to the server team.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Change the password for the relevant account in the related database program;
2. Discuss with groups to see if changes to process and documentation is required;
3. Establish extent of condition;
4. Update and publish any required document revisions;
5. Validate all asset password last-changed dates are synced with the relevant database program; and
6. Create a checklist for adding a new account in the relevant database program and validating the last change.

URE certified that all mitigation actions were completed.

CIP-007-3a R6 (RFC2015015107) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, when URE commissioned four devices they inadvertently created firewall rules that disallowed logging.

ReliabilityFirst determined the duration of the violation to be approximately one month, from the date URE commissioned the devices, to the date the devices began sending logs to the logging tool.

The issue occurred because of a hierarchy issue where a different device was programed incorrectly and placed higher in the hierarchy, thereby blocking traffic from the four devices. The violation involved the management practices of asset and configuration management and verification. Asset and configuration management was involved because URE failed to manage changes to the devices during the commissioning process. Additionally, verification was involved because URE failed to verify that the firewall rule correction worked as intended prior to commissioning the devices.

ReliabilityFirst determined that this violation posed a minimal risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Terminate the cyber security analyst as a result of not satisfactorily performing his job responsibilities;
2. Determine the extent of condition by verifying that all assets which are defined in CCA lists are sending logs to the logging tool and are associated with the correct groups to generate alerts defined in its related process;
3. Evaluate a solution to monitor the configuration of the logging tool's log sources that controls CIP alerting and test email alerting;
4. Build a new rule in the logging tool to alert the manager of the cyber security department and the director of the networks and information security department after the logging tool has not received logs from a device in 96 hours;
5. Implement a solution to monitor the logging tool's logs;
6. Update the processes and work forms associated with change management and commission to include specific controls an asset administrator must act upon to ensure CIP-005 and CIP-007 controls are addressed in alignment with CIP Version 5;
7. Conduct a training session on newly proposed processes and work forms, and address all applicable Subject Matter Expert (SME) questions and concerns during the page-turn exercise;

8. Correct any findings or deficiencies discovered during the extent of condition analysis conducted in Milestone 2; and
9. Complete a CIP-007 R6 Mitigation Plan closure report.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-007-3a R6 (RFC2016015752) – OVERVIEW

ReliabilityFirst determined that URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, in two instances certain programs were not sending failed login attempt notifications to URE's logging tool.

ReliabilityFirst determined the duration of the violation to be approximately six months, from the date URE failed to monitor logs in the second instance, to the date URE completed its Mitigation Plan.

The violation involved the management practices of asset and configuration management because URE did not adhere to its configuration management process.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Investigate and resolve logging issues with the two relevant programs;
2. Establish a change review board;
3. Implement a certain monitoring program as a change management tool;
4. Train teams on change control process and the new monitoring program;
5. Update relevant documents for asset classes to include specific and proper logging configuration and specific testing measures to prove logging is functional;
6. Perform logging extent of condition assessment to analyze all CIP devices to ensure they are logging to the logging tool properly; and
7. Update any additional relevant documents to include specific and proper logging configuration and specific testing measures to prove logging is functional.

URE certified, and ReliabilityFirst verified, that all mitigation actions were completed.

CIP-014-2 R1 (RFC2015015312) – OVERVIEW

ReliabilityFirst determined that URE failed to perform an initial risk assessment and subsequent risk assessments of its transmission stations and transmission substations that meet the criteria specified in CIP-014-2. Specifically, URE did not assess one substation pursuant to Section 4.1.1 of the CIP-014-2.

ReliabilityFirst determined the duration of the violation to be approximately five days, from the date URE was required to comply with CIP-014-2 R1, to the date URE completed its risk assessment for the substation at issue.

The major contributing cause was a change to the baseline list of substations used during the evaluation process occurred (to add the substation) and was not communicated to those conducting the assessment. The violation involved the management practice of verification because URE failed to verify that each qualifying substation would be reviewed in compliance with CIP-014.

ReliabilityFirst determined that this violation posed a moderate risk to the reliability of the BPS.

URE submitted a Mitigation Plan to address the referenced violation, and committed to the following actions:

1. Perform a review of applicability Section 4.1.1 and identify all missing substations;
2. Perform risk assessments for missing substations;
3. Include a planning SME as a reviewer of CIP-002-5 BES Cyber Asset identification process results; and
4. Revise the CIP-014 R1 planning process to include a secondary review of the list of applicable substations to confirm it is complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, ReliabilityFirst has assessed a penalty of one hundred eighty thousand dollars ($180,000) for the referenced violations.

In reaching this determination, ReliabilityFirst considered the following factors:

1. URE had relevant prior violations of CIP-007-3a R2 and R5;
2. URE had an internal compliance program at the time of the violation, which was considered a mitigating factor in penalty determination;
3. URE self-reported 20 of the violations;

4. URE was highly cooperative throughout the compliance enforcement process;
5. there was neither evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. fifteen of the violations posed a minimal risk, six of the violations posed a moderate risk, and one violation posed a serious and substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, ReliabilityFirst determined that, in this instance, the penalty amount of one hundred eighty thousand dollars ($180,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the violations on May 8, 2018 and approved the terms of the Settlement Agreement. In approving the terms of the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

For the foregoing reasons, the NERC BOTCC approved the terms of the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Jason Blake* General Counsel & Corporate Secretary ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 jason.blake@rfirst.org (216) 503-0683 (216) 503-9207 facsimile Kristen M. Senk* Managing Enforcement Counsel ReliabilityFirst Corporation 3 Summit Park Drive, Suite 600 Cleveland, OH 44131 kristen.senk@rfirst.org (216) 503-06769 (216) 503-9207 – facsimile *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Robert Goldfin* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile robert.goldfin@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Robert P. Goldfin

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Robert P. Goldfin
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
robert.goldfin@nerc.net

cc: Unidentified Registered Entity
ReliabilityFirst Corporation

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 31, 2018

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP18-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction, or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and materials:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
2	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2017016850	Settlement Agreement

	F	G	H	I
1	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**
2	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-004-6 R5 Part 5.1. Specifically, WECC_URE1 reported two instances where it did not adequately implement its process to complete the removal of unescorted physical access within 24 hours of a termination action. In the first instance, a service contractor employee with unescorted physical access to WECC_URE1's Medium Impact BES Cyber Systems (MIBCS) was terminated. WECC_URE1 was not notified by the contract vendor within four hours of the termination, per its contract with the vendor. WECC_URE1 processed the termination within 24 hours of receiving the termination notice, which was approximately 36 hours after the termination action taken by the contract vendor. The second instance occurred when a service contractor employee with unescorted physical access to WECC_URE1's MIBCS was terminated. WECC_URE1 did not revoke access within 24 hours after the termination action, because the contract vendor did not send the termination email to the correct email address and the WECC_URE1 offices were closed for the Thanksgiving holiday. WECC determined that on two separate instances, WECC_URE1 failed to revoke unescorted physical access to its MIBCS for two contract employees within 24 hours of the termination action. The root cause of the first instance was a vendor contractor not performing according to the contract language; and for the second instance was a less than adequate vendor contract, thereby delaying the access revocation process. Specifically, the vendor contract contained an outdated version of a clause which did not specify a method of communicating termination actions to WECC_URE1.	CIP-004-6	R5; Part 5.1	Medium

	J	K	L	M	N
1	**Violation Severity Level**	**Risk Assessment**	**Violation Start Date**	**Violation End Date**	**Total Penalty or Sanction ($)**
2	High	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In both instances, WECC_URE1 failed to implement a process to initiate removal of an individual's authorization for unescorted physical access upon a termination action and complete the removals within 24 hours of the termination action. Specifically, for two personnel, WECC_URE1 failed to revoke unescorted physical access to its MIBCS within 24 hours of the termination action. Following a termination action, a disgruntled employee or contractor who retains unescorted physical access to substations could make unauthorized changes to the transmission Facilities and equipment by removing them from service; thereby, potentially disabling the System Operator's ability to control the system and disrupting WECC_URE1's ability to fulfill its responsibilities. WECC_URE1 implemented weak controls to prevent the noncompliance from occurring. WECC_URE1 had implemented a Master Contract for service providers that specified the process for communicating a termination; however, all vendor contracts were not updated to the current version of the Master Contract. No controls were identified that would have allowed WECC_URE1 to detect that the vendor contractor took a termination action but did not provide proper notification. The risk was reduced because in both instances, access was granted to MIBCS and the duration of access was very short. Additionally, in both instances, the badge was not used to gain access during the violation duration. Based on this, WECC determined that the potential harm had a moderate likelihood of occurring. No harm is known to have occurred.	first instance of when unescorted physical access should have been revoked	when access was revoked for the last instance	No Penalty

	O	P	Q	R	S
1	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**
2	Self-Report	To mitigate this violation, WECC_URE1: 1) performed a review of service contracts for the applicable revocation clause and clause version and updated accordingly; 2) established a consistent response to vendor contractors who fail to perform revocation notification requirements; 3) reviewed with applicable WECC_URE1 personnel proposed changes to its purchasing instructions; and 4) updated WECC_URE1 policies prior to the next publication.	12/26/2017	1/29/2018	Does Not Contest

	T
1	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	WECC_URE1 did not receive mitigating credit for self-reporting because the Self-Report was submitted 210 days after WECC_URE1 discovered the violation. Credit was not given for WECC_URE1's internal compliance program (ICP). Although WECC_URE1 has a documented ICP that was provided to WECC, WECC determined that WECC_URE1 did not implement its ICP with effective internal controls to prevent or detect this violation in a timely manner. WECC considered WECC_URE1's CIP-004 compliance history to be aggravating in determining the disposition track.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 31, 2018

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP18-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction, or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and materials:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

A-2 Public CIP - Spreadsheet Notice of Penalty Summary

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
2	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2017018459	Settlement Agreement	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-007-6 R2 Parts 2.1, 2.2, 2.3, and 2.4. Specifically, WECC_URE1 reported that it was instructed by the designer, manufacturer, and warranty provider of the high voltage direct current protection and control system (HVDC PCS) at a substation, that its patches and updates for software and firmware provided during the warranty period would be functional patches rather than security patches and only for the designer's proprietary devices. The designer's position was that because the substation Station Control and Monitoring (SCM) network for the HVDC PCS was a private network with no External Routable Connectivity (ERC), it did not perform security patching because of the potential to disrupt operations. Due to a setting in a single device being incorrect, the SCM network suffered a failure during the trial operation phase. The designer's position was not to apply security patches to the system devices because those security patches could pose a risk to system reliability without providing a tangible security benefit. As a term of purchase, the designer had approving authority for implementation of patches for third-party manufactured devices that were utilized by the designer in the system design. Because of this agreement between WECC_URE1 and the designer, the responsibility of evaluating security patches for the third-party devices and Operating System platforms had yet to be defined. The HVDC PCS at the substation was an engineered high speed, real time, closed loop, protection and control system. This engineered system consists of multiple devices running multiple software packages that are closely integrated by the manufacturer, to meet the protection and control requirements. The manufacturer and designer sold the engineered system to WECC_URE1 and retained the knowledge of how the software and hardware integrations work. As required by CIP-007-6 R2 Part 2.1, WECC_URE1 had identified the manufacturer as the patch source for the HVDC PCS at the substation. However, since the manufacturer does not have a website with patching information for the HVDC PCS, it was required to notify WECC_URE1 when new security patches were available. The evaluation of security patches for the BES Cyber Assets (BCAs) and Protected Cyber Assets (PCAs) at the substation and the creation of mitigation plan(s), had not taken place since the requirement became effective on July 1, 2016 as required by CIP-007-6 R2 Parts 2.1, 2.2, 2.3, and 2.4. Additionally, WECC_URE1 was performing its CIP-007-6 R2 security patch management program for the other CIP devices by different manufacturers within this substation. This violation was discovered during WECC_URE1's preparation for a WECC audit. WECC determined that WECC_URE1 failed to implement a program or process for tracking (2.1), evaluating (2.2), and installing cyber security patches or creating a mitigation plan to address the vulnerabilities addressed by each security patch that was not installed (2.3) and implementing the mitigation plan (2.4) for its designer devices at its substation, designated as a Medium Impact BES Cyber Systems (MIBCS), consisting of BCAs and PCAs. WECC determined that this violation began when the Standard and Requirement became mandatory and enforceable for WECC_URE1, and ended when WECC_URE1 implemented a security patch management program for the designer's devices in its MIBCS located at its substation, for a total of 502 days of noncompliance. The root cause of this violation was WECC_URE1's not integrating the substation HVDC PCS into the field patch management process. Specifically, WECC_URE1 underestimated the resources needed and effort required to establish and operate a compliant security patch management program at its substation.	CIP-007-6	R2; P2.1, 2.2, 2.3, and 2.4	High	Severe
3	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2017017974	Settlement Agreement	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-005-1 R2.4. Specifically, WECC_URE1 reported that during a routine audit, it was discovered one Cyber Asset at a substation with External Routable Connectivity (ERC) containing Medium Impact BES Cyber Systems (MIBCS) that allowed access to a relay without any authentication procedure. The investigation showed that the device had been set to allow access without a password. Because this violated the approved configuration for these devices, technical services issued an inspection of all in-service devices to review and correct any devices which were not set up correctly (remote authentication enabled and all ports set to require authentication). WECC_URE1 determined there were no additional devices configuration issues. The improperly configured device had one port where the access control default was not changed to require a password. This setting was changed on the day it was found. This setting change is required in the configuration manual utilized by WECC_URE1 . The manual was also reviewed and additional language was added to reinforce the requirement to enable passwords. WECC determined that WECC_URE1 failed to implement strong procedural or technical access controls at the access point of an Electronic Security Perimeter (ESP) to ensure authenticity of the accessing party for one device that allowed access to a relay. The root cause of this violation was the accuracy or effectiveness of changes were not verified or validated. Specifically, the configuration of the device was never completely validated to ensure accuracy.	CIP-005-1	R2; R2.4	Medium	Severe
4	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2016015839	Settlement Agreement	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-007-3a R3.1. Specifically, WECC_URE1 reported that in preparation an audit, WECC_URE1 determined that it was not able to confirm that it documented the assessment of security patches and security upgrades for applicability within 30 calendars days of the availability of the patches or upgrades for seven Critical Cyber Assets (CCAs). The CCAs included two Remedial Action Schemes (RAS) within its Control Centers and five network servers. During an internal investigation of this noncompliance, WECC_URE1 determined that after experiencing network connection issues, one of its technicians saved evidence of security patch assessment to his computer’s hard drive, which was subsequently wiped clean without saving a copy when the technician’s employment ended; resulting in a gap in security patch management documentation from. After reviewing all relevant information, WECC determined an increase of scope from the initial Self-Report. During scheduled maintenance, WECC_URE1 performed a full investigation which identified 58 additional RAS system devices, and 6 RAS servers. WECC_URE1 failed to document the assessment of security patches and security upgrades for applicability within 30 calendar days of the availability of the patches or upgrades for a total of 71 CCAs. The root cause of the first device issue was the improper identification and classification of a device in the PACS systems. The root cause of the network equipment issue was the poor transition of duties between personnel. The root cause of the RAS system issue was the lack of written communication. Specifically, a specific security patch fix was not documented on WECC_URE1’s patch discovery list.	CIP-007-3a	R3	Lower	Severe

	K	L	M	N	O	P	Q	R	S
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**
2	WECC determined this noncompliance posed a moderate risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. In this instance, WECC_URE1 failed to implement or document a security patch management program for its manufacturer's devices within its MIBCS consisting of BCAs and PCAs, located at the substation, as required by CIP-007-6 R2. Such failure could potentially result in unauthorized electronic access to the vulnerable systems within WECC_URE1's substations. Unauthorized electronic access, due to unpatched software, could result in complete control of the unpatched devices due to malware infection or other successful intrusion into the network locations of the unpatched systems. The result could be complete control (installation of software, exfiltration of data, remote control, etc.) of the affected system and an anchor point for reconnaissance and spreading through the environment, which could result in significant negative effects to the BPS, including neighboring entities via interties. The substation monitors and controls a WECC major path. However, the substation has no ERC to the substation; therefore, any compromise would have to be performed at the physical site itself. WECC_URE1 implemented weak controls to detect this violation. Vendor-approved security patches are applied on an annual basis for vendor-owned CIP assets. All other CIP assets are managed under WECC_URE1's security patch management program. Based on this, WECC determined that the potential harm had a moderate likelihood of occurring.	when the Standard and Requirement became mandatory and enforceable	when a security patch management program was implemented for the devices in scope	No penalty	Self-Report	To mitigate this violation, WECC_URE1: 1) enrolled the BCAs and PCAs at the substation into its firmware tracker; 2) utilized its existing patch mitigation plan process to document all designer-released security patches that needed to be deployed to the devices in scope; and 3) documented changes to the baseline for firmware or software as a result of deploying patches during a maintenance outage.	11/15/2017	12/7/2017	Does Not Contest
3	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, WECC_URE1 failed to ensure authentication at the device access point for all user access into WECC_URE1's substation containing MIBCS as required by CIP-005-1 R2.4. Such failure could result in inappropriate access via a compromised or misused remote access account resulting in significant negative effects on the reliability and stability of the Bulk Electric System (BES), including but not limited to disruption, manipulation, or compromise of the MIBCS for reconnaissance. WECC_URE1 implemented weak detective controls in that the issue was identified as a result of an audit 8 years after the device should have been compliant with the CIP-005-1 R2.4. However, access to device was limited to a small number of personnel who were authorized to have said access. The improper setting allowed direct access to the device from WECC_URE1's network The network requires privileges and authentication to access. This is a local WECC_URE1 network for supporting field BES Cyber Systems that does not have direct access to the Internet. A detailed configuration review of devices revealed no additional misconfigurations. Based on this, the potential harm had a minimal likelihood of occurring.	when access point authentication should have been implemented	when WECC_URE1 implemented access point authentication	No penalty	Self-Report	To mitigate this violation, WECC_URE1 1) changed the configuration on the device to require authentication; 2) reviewed all device configuration to ensure authentication was configured prior to accessing any ESP; 3) updated the device configuration procedure to provide additional emphasis on the setting of port passwords; 4) added an additional control to the device configuration procedure requiring discovered instances of device configuration inconsistent with configuration document to be presorted to the Subject Matter Expert; and 5) sent an email notification to applicable personnel communicating the change to the device configuration procedure.	8/14/2017	1/29/2018	Does Not Contest
4	This violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. In this instance, WECC_URE1 failed to document the assessment of security patches within 30 days for 71 CCAs. Such failure may lead to security exposures that could result in serious adverse effects on WECC_URE1's operations, including the installation of potentially harmful software on the CCAs. Installation of malware or other harmful software could lead to unintended access and eventually to control of systems and software. Given that this violation involved several different locations containing the CCAs, a widespread coordinated attack would be conceivable. As such, the failure to adequately protect devices and resources could affect the reliability of the BPS. However, the controls implemented by WECC_URE1 reduced the likelihood of the potential harm from occurring. Specifically, none of the network equipment has internet access and was secured in server rooms with limited authorized physical access. Additionally, antivirus was maintained on all network applicable devices. The RAS equipment does not have ERC and is also located in locked cabinets within Controls Centers, with alarming for access attempts.	when security patches and security upgrade assessments should have been documented.	Mitigation Plan completion	No penalty	Self-Report	To mitigate this violation, WECC_URE1: 1) updated its patch management plan; 2) assessed for applicability all security patches and security upgrades for the devices in scope; 3) initiated change tickets for security patches and security upgrades assessed as applicable for the devices in scope; 4) updated its processes and procedures for RAS systems patch discovery, evaluation, testing, and installation; 5) ensured all installed software on RAS systems in scope are on the patch source list for monthly discovery and evaluation; and 6) ensured all applicable security patches are part of its RAS system upgrade.	5/15/2017	10/12/2017	Does Not Contest

	T
1	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a neutral factor in the penalty determination. Although WECC_URE1 does have a documented ICP, WECC determined that WECC_URE1 did not implement effective controls to detect this violation in a timely manner. WECC considered WECC_URE1's CIP-007-6 R2 compliance history in determining the disposition track. WECC considered WECC_URE1's compliance history to be an aggravating factor in the penalty determination.
3	WECC did not give credit for WECC_URE1's internal compliance program (ICP). Although WECC_URE1 does have a documented ICP, WECC determined that WECC_URE1 did not implement effective controls to detect this violation in a timely manner. WECC considered WECC_URE1's CIP-005-1 R2.4 compliance history in determining the disposition track. WECC considered WECC_URE1's CIP-005-1 R2 compliance history to be an aggravating factor in the penalty determination.
4	WECC did not give credit for WECC_URE1's internal compliance program (ICP). Although WECC_URE1 does have a documented ICP, WECC determined that WECC_URE1 did not implement effective controls to detect this violation in a timely manner. WECC_URE1 did not receive mitigating credit for self-reporting because the Self-Report was submitted after receiving notice of an upcoming Compliance Audit. WECC considered WECC_URE1's CIP-007-3a R3 compliance history in determining the disposition track. WECC considered WECC_URE1's CIP-007-3a R3 compliance history to be an aggravating factor in the penalty determination.

	A	B	C	D	E	F	G	H	I	J
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**	**Description of the Violation**	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**
5	Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2017017706	Settlement Agreement	WECC_URE1 submitted a Self-Report stating that it was in violation of CIP-006-6 R2 part 2.2. Specifically, WECC_URE1 reported that as part of its reliability compliance monitoring efforts, during an internal spot check of visitor logs it discovered that an entry made on a specific date did not include a last exit time for one visitor as required by CIP-006-6 R2 Part 2.2. WECC determined that WECC_URE1 failed to include all the required elements of CIP-006-6 R2 Part 2.2 specific to one visitor on its visitor log. The root cause of this violation was due to a mental lapse that lead to an incorrect performance. Specifically, the visitor escort was trained appropriately in the process; however, did not follow that process. WECC determined that this violation began when WECC_URE1 did not fill in the last exit time on a visitor log, and ended when WECC_URE1 mitigated this violation, for a total of 372 days of noncompliance.	CIP-006-6	R2; P2.2	Medium	Severe

	K	L	M	N	O	P	Q	R	S
1	**Risk Assessment**	**Violation Start Date**	**Violation End Date**	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**
5	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this instance, WECC_URE1 failed to include all the required elements of CIP-006-6 R2 Part 2.2 specific to one visitor on its visitor log. Such failure could lead to the visitor being allowed back in without knowledge; without justifiable cause; and potentially without a visitor escort. In addition, ensuring that visitors are logged out provides closure of the visitor management process and clarification that the individual is still not somewhere in the facility, which during an emergency could create an issue for security personnel attempting to locate the individual for safety concerns. However, WECC_URE1 implemented good preventive controls. Specifically, WECC_URE1 maintained a visitor escort for the visitor while in the Physical Security Perimeter (PSP), and performed all required duties with the exception of ensuring final logout of the visitor. The PSP which was protecting the control center was manned 24 hours a day, seven days a week by system operators and physical security personnel. Additionally, cards issued to visitors must be turned back in to Security prior to final exit, and the cards do not actually open any access points; thereby, reducing the likelihood of re-entrance without an escort. WECC determined the potential harm had a remote likelihood of occurring.	when the visitor log was not filled in completely	Mitigation Plan completion	No Penalty	Self-Report	To mitigate this violation, WECC_URE1: 1) reiterated to the escort involved with this violation, and other applicable personnel, of the requirement to fill out the visitor log in its entirety when acting as an escort; 2) updated the visitor procedures for its control center to be consistent with the visitor procedures at its other control center, which changes the log from being a physical book that used handwritten updates to log visitors to a digital SharePoint list; 3) modified its procedures to standardize the roles and responsibilities at the control centers; 4) updated the PSP plan to include the revised visitor process that is applicable to both control centers; and 5) sent communications to applicable personnel to establish the revised visitor process at its control center.	6/29/2017	1/31/2018	Does Not Contest

	T
1	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
5	WECC reviewed WECC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. It was through the internal control of monitoring that this violation was discovered. WECC considered WECC_URE1's CIP-006-6 R2 compliance history in determining the disposition track. WECC considered WECC_URE1's compliance history to be an aggravating factor in the penalty determination.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NON-PUBLIC AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

August 30, 2018

VIA ELECTRONIC FILING

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP18-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violation,[3] with the Commission because the Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of a violation of NERC Critical Infrastructure Protection (CIP) Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2018). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

According to the Settlement Agreement, URE admits to the violation and has agreed to actions to mitigate the instant violation and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC).

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2018), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method *SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation						
NERC Violation ID	**Standard**	**Req.**	**VRF/VSL**	**Discovery Method***	**Risk**	**Penalty Amount**
WECC2015015218	CIP-005-3a	R1	Medium/ Severe	CA	Serious	No Penalty

WECC2015015218 CIP-005-3a R1 - OVERVIEW

During a Compliance Audit, WECC reviewed URE's network diagrams and determined that URE was in noncompliance with CIP-005-3a R1. Specifically, WECC discovered that URE failed to accurately identify and document all electronic access points to the Electronic Security Perimeters (ESPs) as required in CIP-005-3a R1. URE used layer 2 switches to segment ESP networks from untrusted non-ESP virtual local area networks (VLANs), creating a mixed-trust environment with possible access to Critical Cyber Assets (CCAs) within the ESP. This mixed-trust environment established external routable connectivity into the ESP without going through an identified Electronic Access Point, contrary to the CIP requirement. WECC was not able to verify the security controls associated with the non-CIP VLANs.

The root cause of this noncompliance was a misinterpretation of the Standard. URE did not consider the layer 2 switches on the non-ESP VLANs as access points to the ESP.

WECC determined that this violation posed a serious risk to the reliability and security of the bulk power system (BPS). In this instance, URE failed to identify and document access points to the ESP as required by CIP-005-3a R1. Specifically, URE utilized layer 2 switches to logically segment ESP networks from untrusted non-ESP VLANs at multiple facilities. Not properly verifying access permissions into the ESP increased the likelihood of an unauthorized user gaining access to URE facilities. This could have potentially resulted in an unauthorized user gaining access to a non-CIP environment and "hopping" VLANs to gain access to CCAs inside the ESP. This could have led to the misoperation of Bulk Electric System (BES) elements.

URE did not have any controls in place to ensure an unauthorized user did not have access to the layer 2 devices from a non-CIP VLAN and gain access to CCAs inside the ESP. Additionally, URE did not have appropriate controls in place to identify when an unauthorized user attempted to gain, or successfully gained, access to ESP assets.

WECC could not confirm the protections or security controls that the logical segmentation on URE's layer 2 switches provided to the CCAs inside the ESPs. NERC's approach to an ESP trusted enclave identified in CIP-005-3 R1 includes the definition of an ESP (the logical border surrounding a network to which BES Cyber Systems are connected) that requires the security controls identified in the CIP Standards, which is a network (layer 3) security control. A layer 2 switch cannot provide these security controls.

WECC determined the duration of the violation to be approximately six and one-half years, from the date the Standard became mandatory and enforceable, through when URE removed the layer 2 switches and access for the non-CIP VLANs was revoked.

URE submitted a Mitigation Plan to address the referenced violation. To mitigate this violation, URE:

1. developed a new supervisory control and data acquisition (SCADA) and operations network design that removes all mixed-trust layer 2 switches;
2. reviewed and received approval on the new design from the SCADA and Compliance departments; and
3. implemented the new design to remove all mixed-trust environment layer 2 switches.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

WECC proposed no monetary penalty for the violation. In reaching this determination, WECC considered the following factors:

1. WECC determined URE's compliance history should not serve as an aggravating factor;
2. WECC did not provide mitigating credit for URE's internal compliance program. URE did not have any detective controls in place that could have helped identify the issues sooner to lessen the violation duration and thereby lessen the risk;
3. URE admitted to the violation;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt by URE to conceal the violation nor evidence of intent to do so;
6. the violation posed a serious risk to the reliability and security of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed would-be penalty.

After consideration of the above factors, WECC determined that, in this instance, no financial penalty is appropriate.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the violation on August 14, 2018, and approved the terms of the Settlement Agreement. In approving the resolution, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violation at issue.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

For the foregoing reasons, the NERC BOTCC approved the terms of the Settlement Agreement and believes that the proposed resolution is appropriate for the violation and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability and security of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the Notice of Penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the Notice of Penalty, upon final determination by FERC.

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

Melanie Frye* President and Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6882 (801) 883-6894 – facsimile mfrye@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz Heather Laws* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Emily Burgis* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile emily.burgis@nerc.net

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Emily Burgis

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Emily Burgis
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
emily.burgis@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

September 27, 2018

VIA ELECTRONIC FILING
Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street NE
Washington, DC 20426

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP18-_-000

Dear Ms. Bose,

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A,[2] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[3]

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Attachment A is an excel spreadsheet.
[3] *See* 18 C.F.R § 39.7(c)(2).

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval in accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2017). Each Reliability Standard at issue in this Notice of Penalty is set forth in Attachment A.

Status of Mitigation[4]

The mitigation activities are described in Attachment A for each respective violation. Information is also provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction, or Enforcement Action Imposed[5]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, Guidance Order; the October 26, 2009, Guidance Order; the August 27, 2010, Guidance Order; and the March 15, 2012, Compliance Enforcement Initiative Order,[6] the violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[4] *See* 18 C.F.R § 39.7(d)(7).
[5] *See* 18 C.F.R § 39.7(d)(4).
[6] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010); *North American Electric Reliability Corporation,* "Order Accepting with Conditions the Electric Reliability Organization's Petition Requesting Approval of New Enforcement Mechanisms and Requiring Compliance Filing," 138 FERC ¶ 61,193 (2012).

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and materials:

a) Spreadsheet Notice of Penalty, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this Spreadsheet NOP:

Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net	Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight North American Electric Reliability Corporation 1325 G Street NW Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile ed.kichline@nerc.net
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations, and orders.

Respectfully submitted,

/s/ Edwin G. Kichline

Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
ed.kichline@nerc.net

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street NW
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

cc: Entities listed in Attachment B

	A	B	C	D	E
1	**Region**	**Registered EntityName**	**NCR**	**NERC Violation ID**	**Notice of Confirmed Violation or Settlement Agreement**
2	Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2017017596	Settlement Agreement

	F
1	**Description of the Violation**
2	NPCC_URE1 submitted a Self-Report stating that it had three instances of noncompliance with CIP-006-6 R1. As part of NPCC_URE1's NERC Reliability Standards compliance program, a compliance concern was submitted by NPCC_URE1 staff and in accordance with NPCC_URE1's procedures, an internal investigation was conducted of the reported incident that revealed a potential noncompliance. The violation started when NPCC_URE1 failed to follow its NERC CIP Physical Security Plan to restrict physical access, monitor and issue an alarm or alert to personnel identified in its Bulk Electric System (BES) Cyber Security response plan within 15 minutes of detecting unauthorized physical access to one (1) Physical Access Control System (PACS). As a result, there was potential unauthorized access to one (1) PACS for multiple periods of time due to the failure to meet Parts 1.6, and 1.7 of CIP-006-6 R1. Specifically, a room door was propped open for approximately 1 hour and 54 minutes. The timeline is as follows: • 0623: Technician #1 with authorized access enters the room • 0624: PACS generated a propped door alarm • 0628: Security Guard acknowledged propped door alarm and cleared from system • 0815: Security Guard noticed door was open on video camera monitoring system and notified security manager • 0818: Security Guard secured the door In another instance, a room door latch was disabled for approximately 7 hours and 38 minutes. During that time, there were seven (7) forced door alarms generated by the PACS signaling the detection of potential unauthorized physical access (entry/exit without the use of the card reader). Security failed to monitor the alarms and notify a member of the incident response team within 15 minutes of detecting unauthorized access. The timeline is as follows: • 0858: Technician #2 with authorized access disabled lock by stuffing material into the communications' room door lock strike plate, which inhibited the door latch from engaging. • 0858 – 1636: Seven (7) forced door alarms were generated by the PACS, signaling the detection of physical entry without the use of the card reader (potential unauthorized access). Security did not respond as required by NPCC_URE1 procedure and failed to notify a member of the incident response team within 15 minutes of detecting unauthorized access. • 1636: Security Guard discovered the disabled latch during a regular patrol and returned the latch to proper service. In another instance, the room door was propped open for approximately 3 hours and 7 minutes. The timeline is as follows: • 0802 – 0845: Five (5) Technicians with authorized access entered the room • 0845: PACS generated a propped door alarm. The Security Guard acknowledged the propped door alarm, and began to investigate via the CCTV system and site intrusion detection system. The Security Guard cleared the alarm. • 1152: Security Guard who was dispatched to investigate found the propped door and secured it. The Security Guard spoke with a NPCC_URE1 electrician (who has authorized unescorted physical access) in the room. The electrician stated that the door was propped open when he arrived and no one else was in the room.

	G	H	I	J	K	L
1	**Reliability Standard**	**Req.**	**Violation Risk Factor**	**Violation Severity Level**	**Risk Assessment**	**Violation Start Date**
2	CIP-006-6	R1: P1.6; P1.7	Medium	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The PACS network switch within the room permits network communication between card reader control panels and the various PACS servers. It could have been physically damaged or taken out of service by not following the proper access process and/or failing to respond to unauthorized access. If this PACS network switch became unavailable, the primary security monitoring workstation location would be unable to communicate with the PACS server/PSP related card panels. However, all panels would continue to be operational using the last known configuration and an alternate PACS monitoring workstation would provide the monitoring capability. The PACS network switch is not in the direct communications path between the PSP related card panels, PACS servers and the alternate PACS monitoring workstation. The entity reduced the risk of a malicious attacker causing harm to the exposed PACS' core network switch by implementing a defense-in-depth security strategy. The PACS core network switch has no graphical user interface and only provides administrative access through a physical console connection and has its unused physical ports disabled. It also has a secure shell configuration requiring appropriate log-in credentials that are maintained as per NERC CIP requirements. The PACS core network switch is located behind three separate restricted physical access control points, which include a perimeter intrusion detection system, vehicle barriers, and CCTV cameras. Security systems are monitored 24x7 by onsite security personnel. Card readers are used to enter the perimeter and the building containing the room at issue. All personnel who can facilitate their own access through the permiter and building must have a valid Personnel Risk Assessment (PRA). All others entering this area are accompanied by personnel having access rights. No other CIP assets are located in the room. During the first two incidents, approximately 30 persons carded into the building. Of those 30, only three (3) did not have access to the room. All three (3) have valid PRAs. During the third incident, approximately 13 persons carded into the building. Of those 13, only four (4) did not have access to the room. All four (4) have valid PRAs, with three (3) having authorized access to other NPCC_URE1 PSPs.	The date the entity failed to follow its NERC CIP Physical Security Plan to restrict physical access, monitor and issue an alarm or alert to personnel identified in its BES Cyber Security response plan within 15 minutes of detecting unauthorized physical access to one PACS.

	M	N	O	P	Q	R
1	**Violation End Date**	**Total Penalty or Sanction ($)**	**Method of Discovery**	**Description of Mitigation Activity**	**Mitigation Completion Date**	**Date Regional Entity Verified Completion of Mitigation**
2	The date the entity resumed following its NERC CIP Physical Security Plan to restrict physical access, monitor and issue an alarm or alert to personnel identified in its BES Cyber Security response plan within 15 minutes of detecting unauthorized physical access to one PACS.	$0	Self-Report	To mitigate this violation, NPCC_URE1: 1) Management conducted an 'on the job briefing' with technicians to reinforce the importance of maintaining physical security; 2) Security conducted refresher training with security management staff to reinforce physical security policies and procedures, including physical access controls; 3) Compliance department referred this matter to NPCC_URE1's labor and law department for employee disciplinary consideration for staff involved in incidents; 4) Security identified and implemented system improvements for forced and propped door alarm notifications and response to unauthorized access to PSPs, specifically, Security worked with an outside vendor to create a PDF window pop-up with specific instructions on when and how to respond to an alarm to help the operator to detect, assess, and respond to alarms; 5) Security and compliance conducted a presentation of physical security policies and procedures during an all-hands meeting; 6) Security implemented new signage for all PSPs at NPCC_URE1's BES facilities to include language related to adherence to NPCC_URE1's physical security procedures; 7) Physical Infrastructure Security increased CCTV recording retention capabilities at all NPCC_URE1 BES facilities; and 8) Physical Infrastructure Security implemented a system for forced and propped door alarm notifications and response to unauthorized access.	12/19/2017	6/25/2018

	S	T
1	**"Admits," "Agrees/Stipulates," "Neither Admits nor Denies," or "Does Not Contest"**	**Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture**
2	Does Not Contest	NPCC reviewed NPCC_URE1's internal compliance program (ICP) and considered it to be a mitigating factor in the penalty determination. NPCC_URE1 self-reported this particular potential non-compliance and continued to be highly cooperative throughout the entire process. Although the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system, NPCC determined that Compliance Exception treatment was not appropriate here based on the underlying conduct, which included deliberate and repetitive actions to prop open a door and/or disable locks in violation of the NPCC_URE1 procedure.