Federal Energy Regulatory Commission
Washington, D.C. 20426

January 21, 2022

FOIA No. FY19-30 (RC13-8)
Fifty Second Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

This is a response to your correspondence received in January 2019, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated January 7, 2022, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC13-8, along with the names of ten (10) relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] Based on my own review of the relevant documents, I conclude that disclosure of these URE identities is appropriate and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC13-8

With respect to the remaining identities of UREs contained in RC13-8, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the

[1] 5 U.S.C. § 552 (2018).

[2] This docket involves multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the UREs for whom FERC initially determined that disclosure of identities may be appropriate.

following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC13-8 will not be disclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney T. Anthony Quinn by email at Tony.Quinn2@usdoj.gov, by phone at (202) 252-7558, or

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2022.01.21 11:23:13 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

Peter Sorenson, Esq.
Counsel for Mr. Mabee
petesorenson@gmail.com

James M. McGrane
Senior Counsel
North American Electric Reliability Corporation
1325 G Street N.W. Suite 600
Washington, D.C. 20005
James.McGrane@nerc.net

Attachment A-2

April 30, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1) **Jo Carroll Energy (JCE)**	NCRXXXXX	MRO2012011576	CIP-002-1	R4	During a Compliance Audit, MRO discovered that MRO_URE1 failed to maintain a signed and dated record of the senior manager or delegate's approval of its annual risk-based assessment methodology (RBAM) for a particular year. In accordance with Standard, the RBAM must be approved annually and have a signed and dated record of the approval. MRO_URE1's current RBAM was approved, signed, and dated approximately one and a half years after its previous RBAM.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The RBAM for the year at issue was approved by the senior manager and in effect, but merely lacked the required signature. The senior manager was not authorized to sign the RBAM and therefore did not do so; however, he has since been delegated the authority to sign the RBAM.	MRO_URE1 current RBAM is approved, signed and dated by the senior manager. MRO has verified the completion of all mitigation activity.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012010235	CIP-004-3	R2; R2.3	NPCC_URE1 self-reported an issue with CIP-004-3 R2.3. The issue was discovered during a recent review by IT Security noting that the vendor had never used his logon-ID. NPCC_URE1 identified one instance where a vendor's annual training had expired and revocation of cyber access was not completed. The vendor was a former employee who was contracted to assist in the resolution of any problems related to NPCC_URE1's energy management system (EMS).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was caused by an automated email notification system failing to make proper notifications. Prior to this incident the former employee's CIP training and personnel risk assessment (PRA) were valid. The former employee did not have physical access to any Critical Cyber Asset's and had "read only" access to one CIP application. The former employee had never used his remote access capabilities to NPCC_URE1's network or his corporate network logon ID. The former employee's responsibility as a vendor was to assist in any troubleshooting or assessment relating to NPCC_URE1's EMS.	To mitigate this issue, NPCC_URE1: 1) did not renew the former employee's contract; 2) updated its procedure to reflect management responsibilities; 3) revised its NERC CIP access management policy, to emphasize the importance of granting CIP access only to "active" employees or vendors; 4) implemented e-mail notifications from the database to IT security and systems security when required CIP training expires for an employee or a vendor; 5) issued a lessons learned document requiring "read and sign" to management who supervise personnel with unescorted CIP physical access or CIP cyber access; 6) developed a test plan that will exercise all CIP critical automated functions to be executed for any future changes impacting the person information database and the associated interfacing systems; and 7) conducted and completed a review of current IT business processes.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012009851	CIP-007-1	R2; R2.1	NPCC conducted a Compliance Audit of NPCC_URE2. NPCC found that NPCC_URE2 had an issue with CIP-007-1 R2.1. NPCC_URE2 listed three ports for Supervisory Control and Data Acquisition (SCADA) host as "unknown" and one port was identified as "Remoteanywhere" and was unable to identify if the ports were required for normal or emergency use. It was determined that the ports were necessary for normal operations.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was due to a documentation oversight. The ports were enabled at the time of the Compliance Audit. The NPCC_URE2 SCADA service vendor monitors the ports and services and ensures that only ports and services necessary for normal or emergency operations are enabled. The ports are associated with the SCADA network which is isolated to the outside by a firewall. The ports reside within the Electronic Security Perimeter and can only be accessed by entering the Physical Security Perimeter with proper authorization to Critical Cyber Assets. The information associated with the ports and services contains data only which is processed through a virtual private network router that is completely disconnected under normal operations. There is no dial-up capability or control circuits associated with these ports and services that can affect BPS operations.	To mitigate this issue, NPCC_URE2; 1) identified and labeled the ports and services prior to the completion of the Compliance Audit; 2) discussed and trained the SCADA service vender on the Mitigation Plan; 3) ensured that only ports necessary for normal or emergency operations are enabled and proper identification of ports and services will be used; 4) will ensure the SCADA administrator will checks the ports and services monthly to verify no unexpected ports and services are running; and 5) will review annually the physical status of ports and services through the vulnerability assessment process.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012010133	CIP-002-3	R3	NPCC conducted a Compliance Audit of NPCC_URE2. NPCC found that NPCC_URE2 had an issue with CIP-002-3 R3. NPCC_URE2 failed to correctly classify and update Critical Cyber Assets (CCA) servers on the approved CCA final listings. The servers provide a conversion from IP-based network traffic to serial-based protocols.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was administrative and due to the entity failing to correctly classify and update CCA's on the approved CCA final listings. These CCAs resided within the Electronic Security Perimeter (ESP) and were also afforded similar protections to those correctly classified CCAs also within the ESP. The servers were not identified on the CCA Summary sheet, but were identified on the NPCC_URE2 CCA assessment list. The servers process system data only and do not contain control circuits that can affect BPS operations.	To mitigate this issue, NPCC_URE2: 1) added both servers to the CCA Summary List; 2) updated the NPCC_URE2 CCA assessment sheet for better readability; and 3) convened the NPCC_URE2 CIP compliance team bi-weekly to address CIP related items and concerns that will help improve its annual vulnerability assessment process.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2013011947	CIP-004-3a	R2; R2.3	NPCC_URE3 self-reported an issue with CIP-004-3a R2.3. NPCC_URE3 discovered that a retired employee did not complete his annual CIP training as a contractor. The retired employee was a former control room supervisor who was hired as a contractor responsible for training distribution operators.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was caused when the company's supervisor failed to re-enroll the contractor in the CIP training program prior to the expiration date. As a former employee the contractor had taken the required CIP training several years in a row and had a current personnel risk assessment (PRA) at the time of the incident. As a contractor, he had unescorted physical access to the Physical Security Perimeter containing Critical Cyber Assets (CCA), but no electronic access to the CCAs. The contractor's function did not involve any capability to affect the operation of the BPS.	To mitigate this issue, NPCC_URE3: 1) had the contractor complete the CIP training; 2) sent an email with a follow-up weekly conference call conveying the process for enrolling both contractors and employees in training; 3) will repeat a CIP reminder of the responsibilities at a semi-annual group meeting of NERC Standards subject matter experts. A weekly conference call is part of a standing agenda item in which the subject matter experts are reminded of various CIP requirements. Each reminder is carried on the agenda for two weeks and is repeated two to three times per year; and 4) will incorporate changes as necessary to the current CIP training policy to clarify the responsibilities of the supervisors and managers.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010190	CIP-003-3	R4.3	NPCC auditors found that NPCC_URE4 had an issue with CIP-003-3 R4.3 because NPCC_URE4 does not conduct an annual assessment that confirms NPCC's full adherence to NPCC_URE4's cyber security plan in documenting the assessment and implementation of actions taken to correct identified deficiencies as required by the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. NPCC_URE4 did provide evidence of an annual review and adherence to information classification that documented test questions, results summary and action items to partially satisfy the Standard.	To mitigate this issue, NPCC_URE4: 1) has an information protection plan (IPP) that has been revised to replace the former assessment practices via quizzes with a new annual assessment process that includes; 2) samples documents subject to the IPP; 3) inspects document printing, copying, and scanning locations to ensure that they have signage posted as reminders of information protection and also have proper marking stamps available to mark documents; and 4) documented assessment results.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010120	CIP-004-3	R4.1	Prior to the beginning of a Compliance Audit, NPCC_URE4 notified the auditors of an issue with CIP-004-3 R4.1. NPCC_URE4 failed to complete a quarterly review of its list of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) on one occasion during the audit period. The quarterly review was performed three weeks late.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. NPCC_URE4's access control program is to deny access by default; no access is granted without going through the proper steps. First, a request is made by the manager of the individual for access. The request must then be approved by the owner. If approved, actual access (physical or electronic) is then granted. This process mitigated the risk that personnel may have access which they should not have before the review was performed. Updates to the list were made at the review. During the gap before the review was performed, a script was run periodically by the applications support team to assist in validating that the access privileges in active directory and certain critical applications were consistent. NPCC_URE4 performed all subsequent quarterly reports as required.	To mitigate this issue, NPCC_URE4: 1) timely completed the next quarterly review of the lists of personnel with access and for the remainder of the audit period; and 2) created workflow to remind managers and other personnel responsible for granting and managing access to complete each quarterly review. The workflow is set to send reminder emails 30 days in advance of the due date and every Tuesday thereafter until the task is marked as complete. Initial implementation provided notification to individuals with a code enhancement later implemented to enable email reminders when more than one individual was assigned a task.

Attachment A-2
April 30, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010188	CIP-007-3	R2	Prior to the beginning of a Compliance Audit, NPCC_URE4 notified the auditors of an issue with CIP-007-3 R2. NPCC_URE4 did not have documentation of ports and services for its Cyber Assets, power distribution units, and media converters, as required by the Standard.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although NPCC_URE4 did not have the documentation of ports and services required by CIP-007-3 R2, it had closed unused ports and services as required by R2's sub-requirements. This issue was documentation only, and the technical controls, i.e., ports and services, were not negatively affected.	To mitigate this issue, NPCC_URE4 created a list of required ports and services for PDUs and Lantronix as well as all other cyber assets within the Electronic Security Perimeter(s) to "establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled."
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010189	CIP-007-3	R5.2	Prior to the beginning of a Compliance Audit, NPCC_URE4 had notified the auditors of an issue with CIP-007-3 R5.2. NPCC_URE4 did not have an approved, documented 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 the Standard.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the NPCC_URE4 did not have the policy required, it had implemented the technical controls required by CIP-007-3 R5.2.1, R5.2.2 and R5.2.3. Accordingly, this issue has minimal impact on the security of the NPCC_URE4 Cyber Assets and thus on the reliability of the BPS.	To mitigate this issue, NPCC_URE4 updated the NPCC_URE4 cyber security policy to include a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010191	CIP-008-3	R1.6	NPCC auditors found NPCC_URE4 had an issue with CIP-008-3 R1.6 because the NPCC_URE4 cyber security incident response plan did not contain any language stating their process for conducting annual tests of the plan as required by the Standard.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the NPCC_URE4 did not contain any language stating their process for conducting annual tests of the plan, NPCC_URE4 was performing and documenting annual tests of the NPCC_URE4 cyber security incident response plan.	To mitigate this issue, NPCC_URE4 updated the NPCC_URE4 cyber security incident reporting and response plan to include the process for conducting annual tests of the cyber security incident reporting and response plan.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5) **Western Electricity Coordinating Council (IA) (WECC IA)**	NCRXXXXX	NPCC2012010707	CIP-002-3	R4	NPCC auditors found NPCC_URE5 had an issue with CIP-002-3 R4 because the NPCC_URE5 senior manager signatory approval for both the Critical Assets and Critical Cyber Asset (CCA) listings did not occur within the allotted annual time frame.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The signatory approval was late, however the review of the Critical Asset and CCA list occurred on time.	To mitigate this issue, NPCC_URE5: 1) completed the signatory approval of the NPCC_URE5 Critical Asset and CCA lists; and 2. created workflow to remind CIP senior manager to review, approve, sign, and date the Critical Asset and CCA lists within the annual timeframe.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010062	CIP-006-3c	R1; R1.6	NPCC_URE6 self-reported an issue with CIP-006-3c R1.6. NPCC_URE6 discovered that an authorized control center employee accompanied by two minor family members entered the energy control center (ECC). The family members were not processed as visitors in accordance with the NPCC_URE6 access control procedure. The visitors' entry and exit were not logged.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The visitors were continuously escorted by a control center employee who had authorized access. At the time of the incident, the authorized control center employee was up to date on all related CIP training and had a current personnel risk assessment.	To mitigate this issue, NPCC_URE6: 1) ECC personnel have participated in a review of current the access control procedure; 2) control center operations and corporate security have installed new security controls at the ECC and alternate control center. These additional controls include a turnstile system that in addition to the existing access controlled doors at the ECC. The turnstiles will be card-access controlled, and will provide an additional layer of physical security, and enhanced capabilities of access monitoring and enforcement; 3) made the necessary updates to its access control procedure, and security plan; 4) trained all relevant personnel on the operation of the new security system and updated procedures; and 5) incorporated the updated plans and procedures into the annual re-training of all employees who have authorized access.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC2012010427	CIP-006-3c	R1, R1.6	NPCC_URE6 self-reported an issue with CIP-006-3c R1.6. An NPCC_URE6 employee who did not have authorized (unescorted) access to the NPCC_URE6 energy control center (ECC) was granted access to the ECC, but was not processed as a visitor in accordance with the access control procedure. The visitor's entry and exit were not logged accordingly.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The employee was allowed to enter the ECC to conduct company business and was continuously escorted by a control center employee who had authorized access at the time of the incident.	To mitigate this issue, NPCC_URE6: 1) ECC personnel have participated in a review of current the access control procedure; 2) control center operations and corporate security have installed new security controls at the ECC and alternate control center. These additional controls include a turnstile system that in addition to the existing access controlled doors at the ECC. The turnstiles will be card-access controlled, and will provide an additional layer of physical security, and enhanced capabilities of access monitoring and enforcement; 3) made the necessary updates to its access control procedure, and security plan; 4) trained all relevant personnel on the operation of the new security system and updated procedures; and 5) incorporated the updated plans and procedures into the annual re-training of all employees who have authorized access.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 7 (NPCC_URE7)	NCRXXXXX	NPCC2013011949	CIP-004-3	R2; R2.1	NPCC_URE7 self-reported an issue with CIP-004-3 R2.1. NPCC_URE7 discovered that one employee's annual CIP training had lapsed but was still granted physical access to Physical Security Perimeter (PSP). The employee was granted access to NPCC_URE7 PSPs, but his annual training had expired. The employee's access card had been disabled previously due to a medical leave of absence.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was caused when the employee's supervisor requested NPCC_URE7 corporate security to reactivate the access card and reinstate all CIP clearances that the employee previously had. The employee has been employed with NPCC_URE7 for almost 20 years. He completed CIP training annually and has a current personnel risk assessment (PRA) on file. The employee works as a building mechanic and was only granted physical access to Critical Cyber Assets (CCA).	To mitigate this issue, NPCC_URE7 updated its procedure for granting physical access. Specifically, the email from the NPCC_URE7 security agent to the contract guard account manager requesting access must include the PRA and training dates. Upon receipt, the contract security account manager will conduct an independent verification of the training and PRA dates and will send an email confirmation back to the NPCC_URE7 security agent confirming that access has been granted. Training will be provided to security personnel on the revised process. NPCC_URE7 reviewed the lessons learned with Corporate Security personnel who have involvement in granting physical access. NPCC_URE7 conducted a review of all individuals that have physical access to PSPs to ensure training and PRAs are current.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011105	CIP-005-1	R1; R1.5	During a Compliance Audit, Reliability*First* determined that RFC_URE1 had an issue with CIP-005-3a R1.5. RFC_URE1 has in place security defense appliances (SDA) that constitute Cyber Assets used in the access control and/or monitoring of the electronic security perimeter (ESP). The SDAs allow for only outbound communication from the ESP. A third-party manages the SDAs and receives metadata from a mirrored port within the ESP so it can analyze anomalous patterns to provide an alert to RFC_URE1. While the third-party has full access and control of the SDAs, it is unable to enter or penetrate the ESP. Reliability*First* discovered that for these Cyber Assets, RFC_URE1 failed to afford the protective measures of CIP-004-3 R3 and CIP-007-3 R3, R5, and R6.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. While the third-party has full access and control of the SDAs, it is unable to enter or penetrate the ESP. The third-party could only disable the SDAs which would render them unable to perform its contracted service of providing logging and alerting to RFC_URE1. In addition, RFC_URE1 afforded the SDAs the remaining protective measures in CIP-005-3a R1.	To mitigate this issue, RFC_URE1: 1) gathered additional necessary evidence to demonstrate that the SDAs were afforded the protective measures as specified in CIP-005-3a R1.5; and 2) reviewed procedures regarding SDAs and updated those procedures as necessary.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011120	CIP-007-1	R2; R2.2; R2.3	During a Compliance Audit, Reliability*First* determined that RFC_URE1 had an issue with CIP-007-3 R2. For some of its servers, RFC_URE1 failed to disable services that are not required for normal and emergency operations, as required by CIP-007-3 R2.2. In addition, while RFC_URE1 appropriately implemented compensating measures for a non-required service that could not be disabled, it failed to file a Technical Feasibility Exception (TFE) for this service, as required by CIP-007-3 R2.3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The services that were not disabled were located within the requisite Physical Security Perimeter and behind two-factor enabled firewalls in the electronic security perimeter (ESP) with robust authorizing, validating, and deprovisioning access control procedures. The services had up-to-date anti-malware technology with security patches that were assessed within the requisite 30 days, cybersecurity tested, and then installed. RFC_URE1 performed cybersecurity vulnerability assessments on the services at least annually as required. RFC_URE1 utilizes a managed security services provider to monitor the services and provide alerts of signature-based intrusion events and potential anomalous traffic crossing into and out of the established ESP using the security defense appliances and a log collection infrastructure. This monitoring and alerting is provided 24 hours a day, seven days a week. Key trained and experienced personnel are notified via pager, email, and/or telephone of any alerts, as warranted by the severity level assigned to the alert. For the non-required service for which RFC_URE1 failed to file a TFE, RFC_URE1 also appropriately implemented the compensating measures described above.	To mitigate this issue, RFC_URE1: 1) utilized a cross-functional team of subject matter experts to review, research, and analyze the existing ports and services; 2) reviewed and enhanced the documented justification for all running ports and services; 3) identified the ports and services not needed for normal and emergency operations and which require specific change of status; and 4) identified the schedule for testing and implementing ports and services.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011125	CIP-004-3	R4; R4.2	RFC_URE1 submitted a Self-Report to Reliability*First* identifying an issue with CIP-004-3 R4. An employee from RFC_URE1's affiliate, with authorized physical access to RFC_URE1's Critical Cyber Assets (CCAs) transferred positions to another affiliate, at which time his access to RFC_URE1's CCAs should have been revoked. The transferred employee's supervisor did not promptly enter a security request system ticket to revoke the employee's access or enter a personnel action notice form for the transfer prior to the employee's transfer date, as was required by RFC_URE1 procedures. As a result, RFC_URE1 revoked this employee's access three days later than the seven days required by CIP-004-3 R4.2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. RFC_URE1 discovered this issue when a compliance specialist reviewed a security request system ticket to remove all access and recognized that the employee transfer date exceeded the seven day requirement by three days. RFC_URE1 revoked access promptly after discovering it had not revoked access. In addition, the employee at issue remained a NERC CIP-cleared individual with cybersecurity training and a valid personnel risk assessment. Furthermore, the employee did not actually enter any of the three Physical Security Perimeters, and remained employed by a RFC_URE1 affiliate.	To mitigate this issue, RFC_URE1: 1) removed the transferred employee's access; and 2) sent a special email notice from RFC_URE1's CIP senior manager to RFC_URE1 supervisors to remind them that when an employee or contract worker no longer requires access to a NERC CIP restricted area or asset, the supervisor is responsible for immediately initiating a ticket to remove the applicable accesses.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011275	CIP-005-3a	R1	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3a R1 to Reliability*First*. While conducting an independent verification of the security patches being installed on certain Cyber Assets, the UREs discovered that it inadvertently installed a system management client on five electronic access control system Cyber Assets, which are Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter (ESP). The Cyber Assets at issue were two-factor authentication servers and firewall policy manager servers that protect physical access control system servers. The UREs installed this client without completing the steps set forth in its change and configuration management control process, as required by CIP-003-3 R6. The UREs did not issue infrastructure change requests for the change associated with deploying the client on those five Cyber Assets due to miscommunications between the personnel responsible for the change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The UREs had tested and installed the client at issue on many other non-CIP protected assets as part of an operating system patching cycle. The UREs observed no adverse consequences resulting from the installation of the client on these assets. The Cyber Assets at issue have numerous protections in place, including being located within a Physical Security Perimeter, up-to-date security patching, monitoring and logging, anti-malware, strong logical access controls, and cyclical cyber vulnerability assessments.	To mitigate this issue, the UREs: 1) uninstalled the client by following the appropriate steps set forth in the change and configuration management control process; 2) counseled the personnel in the responsible workgroup with primary responsibility for servers regarding the importance of following appropriate change management procedures for NERC CIP protected assets and the consequences of not doing so; and 3) conducted a workgroup meeting to reinforce the requirement to document change control and configuration management procedures and processes.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011276	CIP-005-3a	R1	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3a R1 to Reliability*First*. While conducting an independent verification of the security patches being installed on certain Cyber Assets, the UREs discovered that it inadvertently installed a system management client on five electronic access control system Cyber Assets, which are Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter (ESP). The Cyber Assets at issue were two-factor authentication servers and firewall policy manager servers that protect physical access control system servers. The UREs installed this client without completing the steps set forth in its change and configuration management control process, as required by CIP-003-3 R6. The UREs did not issue infrastructure change requests for the change associated with deploying the client on those five Cyber Assets due to miscommunications between the personnel responsible for the change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The UREs had tested and installed the client at issue on many other non-CIP protected assets as part of an operating system patching cycle. The UREs observed no adverse consequences resulting from the installation of the client on these assets. The Cyber Assets at issue have numerous protections in place, including being located within a Physical Security Perimeter, up-to-date security patching, monitoring and logging, anti-malware, strong logical access controls, and cyclical cyber vulnerability assessments.	To mitigate this issue, the UREs: 1) uninstalled the client by following the appropriate steps set forth in the change and configuration management control process; 2) counseled the personnel in the responsible workgroup with primary responsibility for servers regarding the importance of following appropriate change management procedures for NERC CIP protected assets and the consequences of not doing so; and 3) conducted a workgroup meeting to reinforce the requirement to document change control and configuration management procedures and processes.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012011277	CIP-005-3a	R1	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3a R1 to Reliability*First*. While conducting an independent verification of the security patches being installed on certain Cyber Assets, the UREs discovered that it inadvertently installed a system management client on five electronic access control system Cyber Assets, which are Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter (ESP). The Cyber Assets at issue were two-factor authentication servers and firewall policy manager servers that protect physical access control system servers. The UREs installed this client without completing the steps set forth in its change and configuration management control process, as required by CIP-003-3 R6. The UREs did not issue infrastructure change requests for the change associated with deploying the client on those five Cyber Assets due to miscommunications between the personnel responsible for the change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The UREs had tested and installed the client at issue on many other non-CIP protected assets as part of an operating system patching cycle. The UREs observed no adverse consequences resulting from the installation of the client on these assets. The Cyber Assets at issue have numerous protections in place, including being located within a Physical Security Perimeter, up-to-date security patching, monitoring and logging, anti-malware, strong logical access controls, and cyclical cyber vulnerability assessments.	To mitigate this issue, the UREs: 1) uninstalled the client by following the appropriate steps set forth in the change and configuration management control process; 2) counseled the personnel in the responsible workgroup with primary responsibility for servers regarding the importance of following appropriate change management procedures for NERC CIP protected assets and the consequences of not doing so; and 3) conducted a workgroup meeting to reinforce the requirement to document change control and configuration management procedures and processes.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012011374	CIP-005-3	R1; R1.5	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3 R1 to Reliability*First*. While conducting an internal review, the UREs discovered that it failed to change passwords for five shared accounts annually for one Critical Cyber Asset and four Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter (ESP), and Cyber Assets that authorize and/or log access to the physical security perimeter. This conduct implicated assets subject to the requirements of CIP-007-3 R5.3.3 through CIP-005-3 R1.4 and 1.5, CIP-006-3a R2.2, and CIP-007-3 R5.3.3. Reliability*First* determined that the UREs only had an issue with CIP-005-3 R1.5 in order to avoid duplicative enforcement actions. These accounts are not intended for human login, and instead these accounts are interface or system accounts required or used for system-to-system interaction. Due to this fact, the UREs inadvertently overlooked the annual requirement to change these passwords.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The accounts at issue only affected a small subset of Cyber Assets. During the period of the issue, each account had strong passwords that otherwise complied with the CIP Requirements, and only those individuals who were NERC CIP-cleared with a business need knew the passwords. The UREs protects the Cyber Assets at issue with logical access controls, strong physical and electronic controls, and monitoring, logging, and alerting.	To mitigate this issue, the UREs: 1) changed passwords or decommissioned accounts, where appropriate; 2) held review meetings with personnel who have access and responsibility for password management of these accounts to reinforce their understanding of requirements applicable to these assets; 3) communicated directly and firmly to personnel that documented procedures and CIP controls for password management must be complied with; and 4) reiterated to personnel that noncompliance may result in a disciplinary action.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012011375	CIP-005-3	R1; R1.5	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3 R1 to Reliability*First*. While conducting an internal review, the UREs discovered that it failed to change passwords for five shared accounts annually for one Critical Cyber Asset and four Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter (ESP), and Cyber Assets that authorize and/or log access to the physical security perimeter. This conduct implicated assets subject to the requirements of CIP-007-3 R5.3.3 through CIP-005-3 R1.4 and 1.5, CIP-006-3a R2.2, and CIP-007-3 R5.3.3. Reliability*First* determined that the UREs only had an issue with CIP-005-3 R1.5 in order to avoid duplicative enforcement actions. These accounts are not intended for human login, and instead these accounts are interface or system accounts required or used for system-to-system interaction. Due to this fact, the UREs inadvertently overlooked the annual requirement to change these passwords.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The accounts at issue only affected a small subset of Cyber Assets. During the period of the issue, each account had strong passwords that otherwise complied with the CIP Requirements, and only those individuals who were NERC CIP-cleared with a business need knew the passwords. The UREs protects the Cyber Assets at issue with logical access controls, strong physical and electronic controls, and monitoring, logging, and alerting.	To mitigate this issue, the UREs: 1) changed passwords or decommissioned accounts, where appropriate; 2) held review meetings with personnel who have access and responsibility for password management of these accounts to reinforce their understanding of requirements applicable to these assets; 3) communicated directly and firmly to personnel that documented procedures and CIP controls for password management must be complied with; and 4) reiterated to personnel that noncompliance may result in a disciplinary action.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011376	CIP-005-3	R1; R1.5	RFC_URE1, RFC_URE2 and RFC_URE3 (collectively, the UREs) self-reported an issue with CIP-005-3 R1 to Reliability*First*. While conducting an internal review, the UREs discovered that it failed to change passwords for five shared accounts annually for one Critical Cyber Asset and four Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter (ESP), and Cyber Assets that authorize and/or log access to the physical security perimeter. This conduct implicated assets subject to the requirements of CIP-007-3 R5.3.3 through CIP-005-3 R1.4 and 1.5, CIP-006-3a R2.2, and CIP-007-3 R5.3.3. Reliability*First* determined that the UREs only had an issue with CIP-005-3 R1.5 in order to avoid duplicative enforcement actions. These accounts are not intended for human login, and instead these accounts are interface or system accounts required or used for system-to-system interaction. Due to this fact, the UREs inadvertently overlooked the annual requirement to change these passwords.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The accounts at issue only affected a small subset of Cyber Assets. During the period of the issue, each account had strong passwords that otherwise complied with the CIP Requirements, and only those individuals who were NERC CIP-cleared with a business need knew the passwords. The UREs protects the Cyber Assets at issue with logical access controls, strong physical and electronic controls, and monitoring, logging, and alerting.	To mitigate this issue, the UREs: 1) changed passwords or decommissioned accounts, where appropriate; 2) held review meetings with personnel who have access and responsibility for password management of these accounts to reinforce their understanding of requirements applicable to these assets; 3) communicated directly and firmly to personnel that documented procedures and CIP controls for password management must be complied with; and 4) reiterated to personnel that noncompliance may result in a disciplinary action.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013011666	CIP-006-3c	R2; R2.2	RFC_URE1 self-reported an issue with CIP-006-3c R2 to Reliability*First*. RFC_URE1 maintains control panels to control access to Physical Security Perimeters (PSPs), thereby classifying them as Cyber Assets that authorize and/or log access to the PSP. While troubleshooting the installation of a part on the panel, RFC_URE1 installed firmware on a control panel prior to testing that firmware in accordance with its test procedures pursuant to CIP-007-3 R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. RFC_URE1 had installed the firmware on other non-CIP panels and experienced no issues. In addition, RFC_URE1 stored the firmware on the master server used for access control and alarm monitoring. The technician installing the firmware was aware that RFC_URE1 had previously installed this firmware on other panels and that the firmware was stored on the master server. Furthermore, the panels are located behind firewalls with perimeter logging, monitoring, and alerting in place.	To mitigate this issue, RFC_URE1: 1) performed the testing for the firmware and confirmed that the firmware did not contain any malicious code and was authentic; 2) coached the technician on the need to confirm that all requirements are met before implementing any remedial action during installation; and 3) committed to update appropriate procedures to identify work tasks requiring cybersecurity testing.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) **Calhoun Power Company, LLC (Calhoun)**	NCRXXXXX	SERC2013011910	CIP-002-3	R1	The SERC CIP audit team reported that SERC_URE1 had an issue with CIP-002-3 R1 because it failed to identify and document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. SERC_URE1 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE1 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*, SERC_URE1 believed that it had 24 months to identify and document a RBAM to use to identify its Critical Assets. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE1 was required to have identified and documented a RBAM to use to identify its Critical Assets as of its registration date. SERC determined that SERC_URE1 identified and documented a RBAM to use to identify its Critical Assets approximately one year after SERC_URE1's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity that sold SERC_URE1 its assets provided a letter of attestation that previous versions of its RBAM indicated that there were no Critical Assets or Critical Cyber Assets (CCAs) for the generation assets that SERC_URE1 purchased. In addition, SERC_URE1 created and applied a RBAM and found that it did not have any Critical Assets or CCAs.	To mitigate this issue, SERC_URE1: 1) Developed and applied a RBAM and found that it had no Critical Assets or CCAs; 2) Had its senior manager review and approve the RBAM, Critical Asset list, and CCA list; 3) Developed and approved a procedure covering CIP-002; 4) Developed and approved a preventative maintenance activity to require the RBAM to be applied on an annual basis in order to develop and approve the Critical Asset list and CCA list; and 5) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) **Calhoun Power Company, LLC (Calhoun)**	NCRXXXXX	SERC2012011497	CIP-003-3	R2	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-003-3 R2 because it did not assign a single senior manager with overall responsibility and authority for leading and managing SERC_URE1's implementation of, and adherence to, the CIP Standards (CIP senior manager). SERC_URE1 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE1 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities*, SERC_URE1 believed that it had 12 months to designate a CIP senior manager. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE1 was required to have designated a CIP senior manager as of its registration date of November 22, 2011. SERC determined that SERC_URE1 designated a CIP senior manager approximately one year after SERC_URE1's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1 had an asset manager acting as the CIP senior manager since its registration even though the asset manager was not officially designated as the CIP senior manager. In addition, SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE1: 1) Developed and approved a procedure that gives clear detailed guidance on how to comply with CIP-003; 2) Designated in writing a senior manager responsible for CIP activities; 3) Developed and approved a preventive maintenance activity that requires a monthly review of the CIP-003 procedure to ensure that a senior manager is always designated; and 4) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2) **Cherokee County Cogeneration Partners, LLC (Cherokee)**	NCRXXXXX	SERC2013011914	CIP-002-3	R1	The SERC CIP audit team reported that SERC_URE2 had an issue with CIP-002-3 R1 because it failed to identify and document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. SERC_URE2 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE2 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* , SERC_URE2 believed that it had 24 months to identify and document a RBAM to use to identify its Critical Assets. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE2 was required to have identified and documented a RBAM to use to identify its Critical Assets as of its registration date. SERC determined that SERC_URE2 identified and documented a RBAM to use to identify its Critical Assets approximately one year after SERC_URE2's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity that sold SERC_URE2 its assets provided a letter of attestation that previous versions of its RBAM indicated that there were no Critical Assets or Critical Cyber Assets (CCAs) for the generation assets that SERC_URE2 purchased. In addition, SERC_URE2 created and applied a RBAM and found that it did not have any Critical Assets or CCAs.	To mitigate this issue, SERC_URE2: 1) Developed and applied a RBAM and found that it had no Critical Assets or CCAs; 2) Had its senior manager review and approve the RBAM, Critical Asset list, and CCA list; 3) Developed and approved a procedure covering CIP-002; 4) Developed and approved a preventative maintenance activity to require the RBAM to be applied on an annual basis in order to develop and approve the Critical Asset list and CCA list; and 5) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2) **Cherokee County Cogeneration Partners, LLC (Cherokee)**	NCRXXXXX	SERC2012011496	CIP-003-3	R2	SERC_URE2 submitted a Self-Report to SERC stating that it had an issue with CIP-003-3 R2 because it did not assign a single senior manager with overall responsibility and authority for leading and managing SERC_URE2's implementation of, and adherence to, the CIP Standards (CIP senior manager). SERC_URE2 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE2 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* , SERC_URE2 believed that it had 12 months to designate a CIP senior manager. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE2 was required to have designated a CIP senior manager as of its registration date of November 22, 2011. SERC determined that SERC_URE2 designated a CIP senior manager approximately one year after SERC_URE2's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE2 had an asset manager acting as the CIP senior manager since its registration even though the asset manager was not officially designated as the CIP senior manager. In addition, SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE2: 1) Developed and approved a procedure that gives clear detailed guidance on how to comply with CIP-003; 2) Designated in writing a senior manager responsible for CIP activities; 3) Developed and approved a preventive maintenance activity that requires a monthly review of the CIP-003 procedure to ensure that a senior manager is always designated; and 4) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3) **Citizens Electric Corporation (CEC)**	NCRXXXXX	SERC2013011772	CIP-002-1	R1	SERC_URE3 submitted a Self-Certification stating that it had an issue with CIP-002-1 R1 because it did not have a documented risk-based assessment methodology (RBAM) that met all of the requirements of CIP-002-1 R1 to use to identify its Critical Assets. SERC_URE3 had a documented RBAM in place prior to the time that the Standard became mandatory and enforceable, but the initial RBAM lacked evaluation criteria and did not consider any of the assets listed in R1.2.1 through R1.2.7. Subsequent revisions of SERC_URE3's RBAM lacked evaluation criteria and/or failed to consider all of the assets listed in R1.2.1 through R1.2.7.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3 conducted several assessments to determine whether it had Critical Assets and found none, even though those assessments did not include evaluation criteria and/or all the assets listed in R1.2.1 through R1.2.7, as required by the Standard. In addition, SERC_URE3 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE3: 1) Revised SERC_URE3's RBAM to specifically address each and every requirement set forth in CIP-002 R1; and 2) Applied the revised RBAM and had the senior manager approve and sign the RBAM and resulting Critical Assets and Critical Cyber Assets list.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3) **Citizens Electric Corporation (CEC)**	NCRXXXXX	SERC2012011642	CIP-003-1	R2	SERC_URE3 submitted a Self-Report to SERC stating that it had an issue with CIP-003-1 R2 because it failed to assign in writing a single senior manager with overall responsibility and authority for leading and managing its implementation of, and adherence to, the CIP Standards. SERC_URE3 discovered the issue during a mock audit that it conducted as part of its internal compliance program. During an internal compliance team meeting, SERC_URE3 had verbally designated its IT supervisor as the single senior manager with overall responsibility and authority for leading SERC_URE3's CIP program. SERC_URE3 did not document this assignment in writing with the name, title, and date of designation.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE3's IT supervisor was acting as the CIP senior manager during the period in question even though SERC_URE3 had not formally assigned the senior manager responsibility to the IT supervisor in writing. In addition, SERC_URE3 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE3: 1) Documented in writing the designation of SERC_URE3's senior manager responsible for implementation of and adherence to Standards CIP-002 through CIP-009; and 2) Adopted a policy requiring an annual review of the written designation to prevent a future issue with CIP-003 R2.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4) **Doswell Limited Partnership (Doswell)**	NCRXXXXX	SERC2013011918	CIP-002-3	R1	The SERC CIP audit team reported that SERC_URE4 had an issue with CIP-002-3 R1 because it failed to identify and document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. SERC_URE4 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE4 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* , SERC_URE4 believed that it had 24 months to identify and document a RBAM to use to identify its Critical Assets. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE4 was required to have identified and documented a RBAM to use to identify its Critical Assets as of its registration date. SERC determined that SERC_URE4 identified and documented a RBAM to use to identify its Critical Assets approximately one year after SERC_URE4's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The entity that sold SERC_URE4 its assets provided a letter of attestation that previous versions of its RBAM indicated that there were no Critical Assets or Critical Cyber Assets (CCAs) for the generation assets that SERC_URE4 purchased. In addition, SERC_URE4 created and applied a RBAM and found that it did not have any Critical Assets or CCAs.	To mitigate this issue, SERC_URE4: 1) Developed and applied a RBAM and found that it had no Critical Assets or CCAs; 2) Had its senior manager review and approve the RBAM, Critical Asset list, and CCA list; 3) Developed and approved a procedure covering CIP-002; 4) Developed and approved a preventative maintenance activity to require the RBAM to be applied on an annual basis in order to develop and approve the Critical Asset list and CCA list; and 5) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4) **Doswell Limited Partnership (Doswell)**	NCRXXXXX	SERC2012011499	CIP-003-3	R2	SERC_URE4 submitted a Self-Report to SERC stating that it had an issue with CIP-003-3 R2 because it did not assign a single senior manager with overall responsibility and authority for leading and managing SERC_URE4's implementation of, and adherence to, the CIP Standards (CIP senior manager). SERC_URE4 registered with NERC after purchasing assets from a registered entity in the SERC Region. The assets purchased by SERC_URE4 were included in the previous owner's CIP program. Due to a misinterpretation of the CIP Standards and the *Implementation Plan for Newly Identified Critical Cyber Assets and Newly Registered Entities* , SERC_URE4 believed that it had 12 months to designate a CIP senior manager. Pursuant to NERC Compliance Process Bulletin #2011-005, SERC determined that SERC_URE4 was required to have designated a CIP senior manager as of its registration date of November 22, 2011. SERC determined that SERC_URE4 designated a CIP senior manager approximately one year after SERC_URE4's registration date.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE4 had an asset manager acting as the CIP senior manager since its registration even though the asset manager was not officially designated as the CIP senior manager. In addition, SERC_URE4 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE4: 1) Developed and approved a procedure that gives clear detailed guidance on how to comply with CIP-003; 2) Designated in writing a senior manager responsible for CIP activities; 3) Developed and approved a preventive maintenance activity that requires a monthly review of the CIP-003 procedure to ensure that a senior manager is always designated; and 4) Notified appropriate personnel of this issue and the corrective actions taken to prevent recurrence.
Southwest Power Pool Regional Entity (SPP RE); Western Electricity Coordinating Council (WECC); Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (SPP RE_URE1, MRO_URE1, WECC_URE1) (Collectively, URE_1)	NCRXXXXX; NCRXXXXX; NCRXXXXX	SPP2012010005; MRO2012011021; WECC2012009994	CIP-007-3	R1; R1.3	URE_1 submitted respective Self-Reports to SPP RE and WECC, identifying an issue with CIP-007-3 R1.3. The Self-Reports was submitted on behalf of URE_1's affiliated registered entities. Approximately four months later, URE_1 filed a Self-Report for CIP-007-3 R1.3 with MRO, on behalf of another affiliated registered entity. URE_1 self-reported that it did not have documented test results for installation of 29 of 160 patches. Of the 29 patches, 6 pertained to asset installation or replacement, and 23 pertained to installation of software patches.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although URE_1 was unable to provide test results of the 29 patches after their installation, URE_1 did have change orders that noted testing took place and that the patches had been installed. The Energy Management System (EMS) staff member responsible for installing the patch updates noted on the change order that there was no CIP impact to the machines that were updated; therefore, the patch installation did not affect existing cyber security controls to Cyber Assets within the Electronic Security Perimeter (ESP). Additionally, URE_1 provided documentation that it did assess the patches in a simulated production system prior to installation and that the installation of the patches would not adversely affect the operation of an existing Cyber Asset. Further, the Cyber Assets and Critical Cyber Assets within the ESP were only accessible to those with authorized physical and electronic access rights.	To mitigate this issue of noncompliance, URE_1 revised its testing procedures to make the testing documentation requirements clearer to affected EMS personnel. URE_1 trained all affected personnel on the new testing procedures. Additionally, URE_1 instituted a process and schedule for internal auditing every six months to review EMS change records and ensure that the new testing procedures are being followed.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP2012009723	CIP-006-1	R1; R1.8	SPP_URE2 submitted a Self-Report to SPP RE identifying an issue with CIP-006-1 R1.8, which requires that protective measures should be afforded in accordance with certain Standards, including CIP-007-1 R2.1 and R2.2. SPP_URE2 was operating with ports enabled on its badge system that were not required for normal or emergency operations. During a cyber vulnerability assessment (CVA), SPP_URE2 identified one port on its badge system that was not required for normal or emergency operations.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The badge system is guarded by SPP_URE2's electronic access point firewalls and an intrusion prevention system (IPS) residing in series with the firewalls. The firewalls are enabled with anti-virus software and block malicious software accordingly. The IPS reinforces and compliments the firewall by preventing inbound malicious traffic that might successfully cross the firewall, and by preventing malicious outbound traffic from crossing back through the firewall. Furthermore, the badge system is also running anti-virus software, thereby providing another layer of protection beyond the IPS and firewalls. Moreover, SPP_URE2 identified no malicious exploitation of the one erroneously enabled port.	SPP_URE2 disabled the erroneously enabled port.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP RE_URE3)	NCRXXXXX	SPP2011008256	CIP-007-1	R8; R8.3	During a CIP Compliance Audit of SPP_URE3, SPP RE determined that SPP_URE3 had an issue with CIP-007-1 R8.3. SPP_URE3 did not include a review of all of the implemented controls for default accounts in its annual cyber vulnerability assessment (CVA) of all Cyber Assets within the Electronic Security Perimeter. Specifically, SPP_URE3 did not review default account controls that included renaming, disabling, and changing default passwords of default accounts.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The controls of renaming or disabling were implemented and documented but were not reviewed as part of the annual CVA. SPP_URE3 did document other controls for default accounts as part of the annual CVA including reviewing password complexity and password age for all user and default accounts.	SPP_URE3 revised its CVA procedures to include a review of all the implemented controls for default accounts. The performance of the 2012 CVA included such a review.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP RE_URE4)	NCRXXXXX	SPP201100466	CIP-007-1	R4	SPP_URE4 submitted a Self-Report to SPP RE, stating that it had an issue with CIP-007-1 R4 because it failed to submit a timely Technical Feasibility Exception (TFE) request. SPP_URE4 could not install anti-virus software on the communication front-end (CFE) devices of its Energy Management System (EMS) because SPP_URE4's EMS vendor did not have anti-virus software available for these devices. Also, the vendor did not recommend that anti-virus protection be implemented on these devices. Subsequently, SPP_URE4 submitted a second Self-Report stating that it had failed to request TFEs for additional devices all of which were part of SPP_URE4's EMS and were located within the Electronic Security Perimeter (ESP). SPP RE consolidated these two Self-Reports into one issue.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SPP_URE4 demonstrated that it had implemented compensating measures for all of its EMS devices for the duration of the issue. These compensating measures included prohibiting direct Internet connection or email accounts on the EMS, as well as disabling the auto-run and auto-play features on all EMS windows equipment. Additionally, SPP_URE4 had documented the aforementioned compensating measures for its CFE devices, EMS servers, and EMS workstations.	SPP_URE4 submitted TFE requests for all affected devices, and performed the compensating measures it had documented in the TFEs. These TFEs were approved by SPP RE. Additionally, SPP_URE4 terminated two TFEs because it became technically feasible to perform the required actions. SPP_URE4 also updated its anti-virus policy and procedure documents, and trained personnel on the updates.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 5 (SPP RE_URE5)	NCRXXXXX	SPP2012009704	CIP-007-3	R3; R3.1	SPP_URE5 submitted a Self-Report to SPP RE, stating that it had an issue with CIP-007-3 R3.1. SPP_URE5 failed to document 6% of its assessments of available security patches and security upgrades within thirty calendar days of availability.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). While 6% of the patch and security upgrade assessments were not documented within thirty calendar days, 100% were documented within sixty calendar days of availability. Furthermore, only one critical security patch was released during this time. That patch was released for a browser on an asset that did not have Internet access, thus limiting the risk to the BPS. Finally, SPP_URE5 had other measures to protect the affected assets and devices, including strict firewall rules, electronically reviewing logs, anti-virus prevention tools, and security patches.	SPP_URE5 revised its security patch management program to track and evaluate applicable security patches and security upgrades by performing a blanket assessment of all assets approximately every two weeks, regardless whether a new patch or patch upgrade actually is available.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1) **APX Power Markets, Inc. (APX Power)**	NCRXXXXX	TRE2012010996	CIP-002-3	R4	During a Compliance Audit, Texas RE concluded that TRE_URE1 had an issue with CIP-002-3 R4 because the senior manager did not annually approve its null lists of Critical Assets and Critical Cyber Assets (CCAs). Therefore, TRE_URE1 had an issue with CIP-002-3 R4 for about four months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. Although TRE_URE1 did not annually approve the null lists of Critical Assets and CCAs for a period of about four months, TRE_URE1 did in fact have the documents to demonstrate that it used its risk-based assessment methodology (RBAM) to create these asset lists. The Critical Asset and CCA lists based on the RBAM were null during the pendency of the issue.	To mitigate this issue, TRE_URE1 provided a signed and dated record of the senior manager's approval of the null list of Critical Assets and the null list of CCAs. Texas RE has verified the completion of all mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE2012011041	CIP-005-3a	R1.6	TRE_URE2 submitted a Self-Report stating that it had an issue with CIP-005-3a R1. While conducting an annual cyber vulnerability assessment, TRE_URE2 discovered a non-critical Cyber Asset, which was installed for future communications within the Electronic Security Perimeter (ESP). TRE_URE2 determined the non-critical Cyber Asset had not been identified and documented within the asset management system utilized for maintaining documentation of all interconnected non-Critical Cyber Assets within the ESP, as required by CIP-005-3a R1.6. The duration of this issue was for about ten months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The non-critical Cyber Asset at issue was not connected to additional devices in the ESP. In addition, TRE_URE2 afforded the same protections to the non-critical Cyber Asset that are applicable to all access points and devices in the ESP. Furthermore, the non-critical Cyber Asset was located within a Physical Security Perimeter. Finally, TRE_URE2 conducts an annual discovery scan to identify all Cyber Assets within a given ESP. TRE_URE2 compares the results of this scan to a list of known devices, and then identifies any discrepancies. This process led to the discovery of the non-critical Cyber Asset at issue. Texas RE determined that the instant issue is appropriate for FFT treatment because TRE_URE2 discovered the issue during a self-assessment and self-reported the issue.	To mitigate this issue, TRE_URE2: 1) disconnected the non-critical Cyber Asset from the network and powered it down upon discovery; and 2) updated the non-critical Cyber Asset in TRE_URE2's asset management system. Texas RE has verified the completion of all mitigation activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3) **City of Brenham**	NCRXXXXX	TRE2012009731	CIP-003-3	R2; R2.1	During a Compliance Audit, Texas RE concluded that TRE_URE3 had an issue with CIP-003-3 R2. TRE_URE3 had not assigned a single senior manager, as required by R2. When the senior manager was assigned, he was not identified by name, title and date of designation, as required by R2.1. The TRE_URE3 had an issue with this Standard for about one year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Texas RE determined that this is was a documentation issue because the same individual who was previously reviewing and approving the risk-based assessment methodology (RBAM) and Critical Asset and Critical Cyber Asset (CCAs) lists was later designated as the CIP senior manager. TRE_URE3 was already ensuring that the RBAM and Critical Asset and CCA lists were reviewed and approved by the person considered to be the CIP senior manager, although it had not documented his designation properly. Furthermore, even after the CIP senior manager was properly designated, there was no change to the Critical Asset and CCA lists.	To mitigate this issue, the TRE_URE3 officially designated a CIP senior manager by name, title, and date of designation. The CIP senior manager has also reviewed and approved the RBAM and Critical Asset and CCA lists. Texas RE has verified the completion of all mitigation activities.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013011656	CIP-004-3	R4	WECC notified WECC_URE1 that WECC was initiating the Self-Certification process. WECC_URE1 submitted a Self-Report to WECC stating that it had an issue with CIP-004-3 R4. WECC_URE1 reported that it had hired a contractor and granted the contractor unescorted physical access to Critical Cyber Assets (CCAs). WECC_URE1 reported that the contractor was terminated for cause. WECC_URE1 reported that when it terminated the contractor, it revoked the contractor's physical access to its CCAs but did not remove the contractor from its CCA access list. WECC_URE1 reported that it did not remove the contractor from its CCA access list until five months later when it conducted an internal compliance audit. WECC_URE1 reported that it subsequently updated its CCA access list to reflect the termination.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE1, upon releasing the contractor, immediately revoked his identification and access granting badge which is required to physically access WECC_URE1's CCAs. Without an identification badge, WECC_URE1 would have required the contractor to have an escort while interacting with its CCAs. Additionally, all the facilities to which the contractor had access, are continuously monitored by video.	To mitigate this issue WECC_URE1 removed the terminated contractor from its CCA access list.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102930	CIP-007-1	R5	WECC_URE2 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R5. In its Self-Report, WECC_URE2 stated that it performed an incomplete review of individual and shared accounts. WECC_URE2 stated that it failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity that minimizes the risk of unauthorized system access. Specifically, for Cyber Assets located in an Electronic Security Perimeter (ESP), WECC_URE2 failed to implement controls to manage accounts as required by CIP-007-1 R5.1. In addition, for the same Cyber Assets, WECC_URE2 failed to implement a policy to manage use for shared and generic accounts as required by CIP-007-1 R5.2. Finally, for different Cyber Assets located in ESPs, WECC_URE2 failed to change the password at least annually, as required by CIP-007-1 R5.3.3. WECC_URE2 submitted Technical Feasibility Exceptions (TFE(s)) for CIP-007-1 R5. WECC determined that it is technically infeasible for WECC_URE2 to provide adequate password length for the above devices. WECC_URE2 failed to submit TFEs by the due date for submitting TFE Requests. WECC approved the TFEs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). During the issue period, there were a number of compensating measures in place to secure the devices against misuse or malicious attack. All devices were secured within a Physical Security Perimeter (PSP) and then an ESP with a card access system. All individuals must have an authorized card to access the PSP and ESP. In addition, WECC_URE2 stated that controls are implemented to log and monitor access to all Cyber Assets within the ESP and the physical and electronic alerts are reviewed 24 hours a day. For the devices in which it is technically infeasible to implement security controls, WECC_URE2 has additional measures in place to ensure the reliability of the BPS. For example failure of a device will not disable the control operator's visibility. Failure to dispatch in normal configuration has minimal impact. On-site electricians would dispatch the unit manually if necessary restoring operations in a matter of hours.	To mitigate this issue, WECC_URE2: 1) created unique device identifiers for each device for ease of tracking in data collection; 2) reviewed and updated individual, shared, and administrator accounts for all devices in scope; 3) updated passwords for all devices in scope; and 4) submitted TFE requests for the devices incapable of providing adequate password length. WECC approved the TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201102931	CIP-007-1	R6	WECC_URE2 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R6. In its Self-Report, WECC_URE2 stated that it had an inadequate security monitoring and log review in place. WECC_URE2 stated that it failed to implement security controls to monitor cyber security system events. As a result, WECC_URE2 failed to issue alerts for detected cybersecurity incidents, as well as, maintain, retain, and review logs related to security events. The Cyber Assets in scope are used in the access control and monitoring of WECC_URE2's Physical Security Perimeter.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). During the issue period, there were a number of compensating measures in place to secure the devices against misuse or malicious attack. All devices were secured within a Physical Security Perimeter (PSP) and then an ESP with a card access system. All individuals must have an authorized card to access the PSP and ESP. In addition, WECC_URE2 stated that controls are implemented to log and monitor access to all Cyber Assets within the ESP and the physical and electronic alerts are reviewed 24 hours a day. For the devices in which it is technically infeasible to implement security controls, WECC_URE2 has additional measures in place to ensure the reliability of the BPS. For example, failure of a device will not disable the control operator's visibility. Failure to dispatch in normal configuration has minimal impact. On-site electricians would dispatch the unit manually if necessary restoring operations in a matter of hours.	To mitigate this issue, WECC_URE2: 1) created unique device identifiers for each device for ease of tracking in data collection; 2) reviewed and maintained logs per CIP-007-1 R6 for all devices in scope; and 3) submitted TFE requests for the two devices. WECC approved the TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201102923	CIP-007-1	R5	WECC_URE3 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R5. In its Self-Report, WECC_URE3 stated that it performed an incomplete review of individual and shared accounts. WECC_URE3 stated that it failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity that minimizes the risk of unauthorized system access. Specifically, for certain Cyber Assets, WECC_URE3 failed to implement controls to manage accounts. In addition, for the same Cyber Assets, WECC_URE3 failed to implement a policy to manage use for shared and generic accounts. Finally, for the same Cyber Assets and additional Cyber Asset, WECC_URE3 failed to change the password at least annually. The Cyber Assets in scope are located in Electronic Security Perimeters (ESPs). WECC_URE3 submitted Technical Feasibility Exceptions (TFEs) for CIP-007-1 R5. WECC_URE3 failed to submit a TFE by the due date for submitting TFE Requests.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). During the issue period, there were a number of compensating measures in place to secure the devices against misuse or malicious attack. All devices were secured within a Physical Security Perimeter (PSP) and then an ESP with a card access system. All individuals must have an authorized card to access the PSP and ESP. In addition, WECC_URE3 stated that controls are implemented to log and monitor access to all Cyber Assets within the ESP and the physical and electronic alerts are reviewed 24 hours a day. For the devices in which it is technically infeasible to implement security controls, WECC_URE3 has additional measures in place to ensure the reliability of the BPS. For example failure of a device will not disable the control operator's visibility. Failure to dispatch in normal configuration has minimal impact. On-site electricians would dispatch the unit manually if necessary restoring operations in a matter of hours.	To mitigate this issue, WECC_URE3; 1) created unique device identifiers for each device for ease of tracking in data collection; 2) reviewed and updated individual, shared, and administrator accounts for all devices in scope; 3) updated passwords for all devices in scope; and 4) submitted TFE requests for the devices incapable of providing adequate password length. WECC approved both TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201102924	CIP-007-1	R6	WECC_URE3 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R6. In its self-report, WECC_URE3 stated that it had an inadequate security monitoring and log review in place. WECC_URE3 stated that for several of its Cyber Assets, it failed to implement security controls to monitor cyber security system events. As a result, WECC_URE3 failed to issue alerts for detected cybersecurity incidents, as well as, maintain, retain, and review logs related to security events. These devices are located in Electronic Security Perimeters (ESPs).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). During the issue period, there were a number of compensating measures in place to secure the devices against misuse or malicious attack. All devices were secured within a Physical Security Perimeter (PSP) and then an ESP with a card access system. All individuals must have an authorized card to access the PSP and ESP. In addition, WECC_URE3 stated that controls are implemented to log and monitor access to all Cyber Assets within the ESP and the physical and electronic alerts are reviewed 24 hours a day. For the devices in which it is technically infeasible to implement security controls, WECC_URE3 has additional measures in place to ensure the reliability of the BPS. For example failure of a device will not disable the control operator's visibility. Failure to dispatch in normal configuration has minimal impact. On-site electricians would dispatch the unit manually if necessary restoring operations in a matter of hours.	To mitigate this issue, WECC_URE3; 1) created unique device identifiers for each device for ease of tracking in data collection; 2) reviewed and updated individual, shared, and administrator accounts for all devices in scope; and 4) submitted TFE requests for the devices. WECC approved both TFEs.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012009523	CIP-004-3	R4	WECC_URE4 submitted a Self-Certification stating that it had an issue with CIP-004-3 R4. Specifically, WECC_URE4 reported that employees retired who had physical access to Critical Cyber Assets (CCAs) within the Physical Security Perimeters (PSP). WECC_URE4 noted that the individuals in scope were required to have physical access to the PSPs as part of their job duties, but not electronic access to CCAs. At the time these four individuals retired, WECC_URE4 was relocating all of its employees to a new facility. During this time, WECC_URE4 was shifting over to a new physical access control system which was not yet tied in electronically to the configuration management database. WECC_URE4's revocation process consists of automated revocation of logical perimeter access and an electronic update of the access list upon processing an employee for termination. However, during the relocation, the Human Resource Department manually revoked the individuals' access privileges, but, the automated controls were not available to ensure revocation of physical CCA access and comprehensive updating of lists upon termination.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the individuals in scope of the issue had physical access, they did not have electronic access to CCAs. Moreover, physical access was monitored by human observation continuously including security video monitoring. Furthermore, although WECC_URE4 did not update its access list, WECC_URE4 did revoke the individuals' access privileges. Finally, this issue occurred during a construction phase for WECC_URE4, and during this time, WECC_URE4 assigned a dedicated security resource to oversee physical access beyond the typically assigned security.	To mitigate this issue, WECC_URE4: 1) revoked access to four retired employees; 2) updated access list to remove retired individuals; 3) completed logical connection between Human Resource databases; and 4) consolidated database evidence. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011780	CIP-006-3c	R2.1	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-006-3c R2.1. WECC_URE5 reported that an employee was inadvertently granted physical access rights to Cyber Assets provisioning physical access control (PAC) to Physical Security Perimeters (PSPs). An employee was granted physical access to rooms containing PAC devices. Access was granted when a new ID card was being issued to a WECC_URE5 employee. While activating the card, WECC_URE5 staff inadvertently granted physical access rights using a "drop-down" menu in WECC_URE5's physical access control system. The employee did not use this access. WECC_URE5 detected the error and revoked the access rights.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The scope of the issue is limited to a single employee who maintained physical access to devices for a period of less than a month. The PACs devices to which the individual was granted access were secured in rooms that logged and monitored all physical access attempts. Although the employee did not attempt to access either rooms during the duration of the issue, if the employee had attempted to gain access, WECC_URE5 had additional protections in place. The devices to which the employee was granted access were electronically secured. The devices were afforded the protections described under CIP-006-3 R2.2. Specifically, electronic access to the devices required a password. Any attempt by the employee to modify settings to the PACs devices would have triggered alarming. The employee did not have electronic access to the devices.	To mitigate this issue, WECC_URE5modified its physical access control system to reduce the likelihood that access would be inadvertently granted in the future and met with all individuals with administrate privileges to review access grant procedures.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 6 (WECC_URE6)**First Wind O&M, LLC (FWOM)**	NCRXXXXX	WECC2013012073	CIP-002-3	R1	WECC_URE6 submitted a Self-Certification to WECC stating that it had an issue with CIP-002-3 R1. Specifically, WECC_URE6 reported that it changed its Critical Asset identification methodology from a risk-based assessment methodology to a bright-line criteria methodology. WECC_URE6 reported that it later learned that the change in methodology resulted in an issue of CIP-002-3 R1. Under each methodology applied, WECC_URE6 had a null list of Critical Cyber Assets (CCAs).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The potential risks to the BPS were minimized due to compensating measures in place during the duration of the issue. Prior to WECC_URE6 accepting the bright-line criteria methodology, WECC_URE6 applied a risk-based assessment methodology and properly identified its Critical Assets. Furthermore,-WECC_URE6's application of its bright-line criteria methodology produced a list of Critical Assets identical to that created by its previous risk-based assessment methodology. Additionally, the bright-line criteria methodology implemented by WECC_URE6 included proper procedures and considered all asset types as required by CIP-002. Finally, WECC_URE6 does not have CCAs associated with its identified Critical Assets.	To mitigate this issue, WECC_URE6 adopted a new risk-based assessment methodology to identify its Critical Assets as required by CIP-002.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 7 (WECC_URE7)	NCRXXXXX	WECC2013011952	CIP-007-1	R5	WECC notified WECC_URE7 that WECC would be conducting an on-site Compliance Audit at WECC_URE7's office (Audit Notice). After WECC sent the Audit Notice, but prior to WECC's arrival for the on-site Compliance Audit, WECC_URE7 submitted a Self-Report stating that it had an issue with CIP-007-1 R5. In the Self-Report, WECC_URE7 stated that one of its Critical Cyber Assets (CCAs) was not capable of having a password of more than four characters as required by CIP-007-1 R5.3.1. WECC_URE7 reported that the device had not been included in its previously filed technical feasibility exception (TFE).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In this case, the potential risks associated with the issue were minimized due to WECC_URE7's compensating measures. The device in scope is located within an Electronic Security Perimeter (ESP) and a Physical Security Perimeter (PSP) that have limited access. Access to the ESP and PSP is only authorized for personnel who have received CCA training and have undergone a personnel risk assessment. Additionally, the password that existed on the devices was a combination of alpha, numeric, and "special" characters and was changed annually. Finally, the network attached to the device is electronically monitored continuously and if suspicious traffic occurs an alert is immediately sent to WECC_URE7 staff.	To mitigate this issue, WECC_URE7 filed a TFE for the device in question and updated its CIP structured query language database.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 8 (WECC_URE8)	NCRXXXXX	WECC2012011330	CIP-006-3a	R2	WECC performed a Compliance Audit of WECC_URE8 which included auditing compliance with CIP-006-3a R2. During the course of the Compliance Audit, the Audit Team requested security testing evidence on physical access control systems (PACS) servers. WECC_URE8 made significant changes (upgrades) to the servers used in the access control and monitoring of the Physical Security Perimeters (PSPs), and failed to provide the protection of CIP-007 R1 (security testing) as required by CIP-006 R2.2. Based on WECC_URE8's insufficient testing evidence, the Audit Team conducted an interview to discuss what cyber security test procedures WECC_URE8 currently had in place. During the interview, WECC_URE8 stated that it performed functional testing (done at the vendor location on a test server) upon making changes or implementing upgrades to the PACS servers; however, cyber security control testing was not addressed. Because WECC_URE8 did not provide security testing prior to installing the upgrades, WECC_URE8 failed to provide the protection of CIP-007 R1 to the servers, as required by CIP-006 R2.2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although WECC_URE8 failed to perform security testing on the PACS servers, it did perform functional testing prior to installation. Additionally, the PACS servers are located on a protected network with firewall protection and continuous logging and monitoring of cyber access. Also, WECC_URE8 performs annual cyber vulnerability assessments on this protected network, and the PACS servers have antivirus installed.	To mitigate this issue, WECC_URE8: 1) set up a dedicated test server for PACS Cyber Assets to allow functional testing with the vendor and to facilitate testing of the cyber security controls; and 2) updated its test procedures to ensure that the PACS testing are performed consistently on the test system and on the production system. This process includes ensuring that the associated evidence is captured.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 9 (WECC_URE9) **Trans Bay Cable LLC (TBAY)**	NCRXXXXX	WECC2012011575	CIP-002-3	R1	WECC conducted an on-site Compliance Audit of WECC_URE9's facilities and determined that WECC_URE9 had an issue with CIP-002-3 R1. WECC_URE9's Critical Asset identification procedure failed to include a risk-based assessment component; instead, WECC_URE9 had correlated the loss, compromise or misuse of asset function of each asset type for its bulk power system (BPS) Critical Asset characteristics, using characteristics defined in CIP-002-4, Attachment 1 (Version 4). The application of this Critical Asset identification procedure generated a null list of Critical Assets. As part of its review, the audit team also reviewed a prior version of WECC_URE9's procedure based on Version 3 of the CIP Standards, the version currently in effect. This Critical Asset identification procedure also returned null lists of Critical Assets and associated Critical Cyber Assets (CCAs). WECC determined WECC_URE9 had an issue of CIP-002-3 R1 for its failure to identify and document a risk-based assessment methodology to use to identify its Critical Assets and its CCAs, compliant with Version 3 of the CIP Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. WECC performed site visits at WECC_URE9's facilities and determined that, as a compensating measure, WECC_URE9 employs air-gapped networks for its control systems. In addition, the networks are not connected to any other network, including the Internet, and only allow internal data transmission. Finally, both methodologies returned null lists for Cyber Assets and associated CCAs.	To mitigate this issue, WECC_URE9 revised its risk-based assessment methodology to include a risk-based assessment component. WECC has verified the completion of all mitigation activity.