Federal Energy Regulatory Commission
Washington, D.C. 20426

December 22, 2021

Re: FOIA No. FY19-30 (RC12-7)
Thirty Sixth 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 November 10, 2021, 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. RC12-7, along with the names of three (3) 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] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC12-7.

With respect to the remaining identities of UREs contained in RC12-7, 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 following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow 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.

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 RC12-7 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,

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: 2021.12.22 12:02:58 -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

Document Accession #: 20120201-5137 Filed Date: 02/01/2012

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC12-7

January 31, 2012

Alexandria Light & Power (ALP)-.pdf page 9

Northern States Power (Xcel Energy) (NSP)-.pdf page 9

Willmar Municipal Utilities (WLMRWL)-.pdf page 9

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

Re: NERC FFT Informational Filing
FERC Docket No. RC12-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 30 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 57 possible violations[5] of 22 Reliability Standards that posed a lesser risk (minimal to moderate) to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A statement of completion of the mitigation activities has been submitted by the respective Registered Entities.

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2). *See also Notice of No Further Review and Guidance Order*, 132 FERC ¶ 61,182 (2010).
[2] Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.
[3] Attachment A is an Excel spreadsheet.
[4] *See* 18 C.F.R § 39.7(c)(2).
[5] For purposes of this document, each matter is described as a "possible violation," regardless of its procedural posture.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

As discussed below, this FFT includes 57 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined enforcement processes for occurrences that posed lesser risk to the BPS.[6] Resolution of these lesser risk possible violations in this reporting format is appropriate disposition of these matters, and will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards.

Statement of Findings Underlying the FFT

The descriptions of the remediated issues and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval by NERC Enforcement staff, under delegated authority from the NERC Board of Trustees Compliance Committee (NERC BOTCC), of the findings reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), each Reliability Standard at issue in this FFT is identified in Attachment A.

Text of the Reliability Standards at issue in the FFT may be found on NERC's website at http://www.nerc.com/page.php?cid=2|20. For each respective remediated issue, the Reliability Standard Requirement at issue is listed in Attachment A.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the possible violations identified in Attachment A have been mitigated. The respective Registered Entity has submitted a statement of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, spot check, random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

[6] *See North American Electric Reliability Standards Development and NERC and Regional Entity Enforcement*, 132 FERC ¶ 61,217 at P.218 (2010)(encouraging streamlined administrative processes aligned with the significance of the subject violations).
[7] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Resolution[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,[9] NERC Enforcement staff under delegated authority from the NERC BOTCC, approved the FFT based upon its findings and determinations, as well as its review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the remediated issues.

Request for Confidential Treatment of Certain Attachments

Certain portions of Attachment A include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard possible violations and confidential information regarding critical energy infrastructure.

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

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

[8] *See* 18 C.F.R § 39.7(d)(4).

[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010).

Attachments to be included as Part of this FFT Informational Filing

The attachments to be included as part of this FFT Informational Filing are the following documents and material:

a) Find Fix and Track Report Spreadsheet, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

A Form of Notice Suitable for Publication[10]

A copy of a notice suitable for publication is included in Attachment C.

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following as well as to the entities included in Attachment B to this FFT:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001 (404) 446-2560 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 david.cook@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

Handling these remediated issues in a streamlined process will help NERC, the Regional Entities, Registered Entities, and the Commission focus on improving reliability and holding Registered Entities accountable for the more serious violations of the mandatory and enforceable NERC Reliability Standards. Accordingly, NERC respectfully submits this FFT as an informational filing.

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001
(404) 446-2560

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
rebecca.michael@nerc.net

cc: Entities listed in Attachment B

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000311	CIP-004-1	R3	During a spot check, FRCC determined that the entity failed to conduct personnel risk assessments (PRAs) in accordance with CIP-004-1 R3. PRAs for five entity personnel with access to entity's Critical Cyber Assets were not conducted within 30 days of personnel being granted access, as required by the Standard. PRAs were delayed between 1 and 5 days. All the risk assessments were completed with no negative results.	FRCC determined that this issue did not pose serious or substantial risk to the reliability of the bulk power system and only posed minimal risk because these PRAs for five long-term entity personnel were delayed between 1 and 5 days. The responsible entity completed the PRAs with satisfactory results. In addition, the personnel had already been submitted to a background check upon hiring. Background checks are performed for all long-term employees at the time of hiring and this background check is similar to one required by the Standard.	The entity completed the mitigation activities for correcting the gaps in the process of conducting PRAs. All late PRAs were conducted with satisfactory results prior to FRCC discovery and FRCC verified the completion of all mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000313	CIP-008-1	R1: R1.4	During a spot check, FRCC determined that the entity failed to maintain a Cyber Security Incident response plan (CSIRP) in accordance with CIP-008-1 R1.4. Specifically, the entity's CSIRP did not include a process for updating the CSIRP within ninety calendar days of any changes, as required by the Standard.	FRCC determined that this issue did not pose serious or substantial risk to the reliability of the bulk power system and only posed minimal risk because during the relevant period there were no changes to the CSIRP. This remediated issue occurred in the very early stages of compliance and was corrected within six months from the compliance date. During this period, no changes were made that could have impacted the CSIRP. Further, the entity promptly mitigated the gap upon discovery.	The entity completed the mitigation activities for correcting the gaps in its CSIRP and included required steps for updating of CSIRP with 90 days from any changes. The issue was resolved prior to FRCC discovery and FRCC verified the completion of all mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC201000411	CIP-004-3	R4; R4.1	The entity self-reported an issue with CIP-004-3 R4.1. The entity self-reported that it did not update the list(s) of personnel with authorized access to Critical Cyber Assets (CCAs) within seven calendar days after the change in access of the personnel with access to CCAs. One staff member was transferred and no longer required access to the CCA, and though his access was revoked, the list of authorized users was not updated within the required seven calendar days. The list was updated six days beyond the required compliance date. The employee was transferred one day before access was revoked, and the database was updated twelve days after the transfer.	FRCC determined that this issue did not pose serious or substantial risk to the reliability of the bulk power system and only posed minimal risk because the entity did not update the list(s) within seven calendar days of the change in personnel with access to CCAs. Since the concerned personnel's access was revoked in a timely manner as required by CIP-004-3 R4.2 and given the fact that this was merely a lack of timely documentation, FRCC concluded that the risk of impact to reliability was minimal. Although the entity has violated this Standard previously, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The entity has four prior violations of CIP-004, three of which involve different requirements and are therefore distinguishable. The prior CIP-004 R4 violation occurred in 2008, nearly three years prior to the issue at hand. Following the prior violation, the entity developed a database for use in tracking and recording training dates and access privileges, reviewed and updated the list of personnel with access to CCAs; reviewed its database; modified its training attendance sheet with a block to indicate database updated for each attendee; created Outlook calendar reminders at four weeks prior to end of the quarter to trigger review process, created a Memorandum of Understanding for contractors to notify the entity of all terminations within 12 hours, reviewed and updated the process for documenting that training has occurred, created a process for Human Resources to notify the energy control center of all employee terminations, and developed queries in the database to facilitate reviews of access lists on a routine basis. The instant remediated issue is distinguishable in that the prior violation involved a lack of documentation of the personnel list review, but the entity did create and maintain the list of authorized users with	The entity promptly completed mitigation activities including updating the list of authorized personnel with access to CCAs, adding another layer of notification from Human Resources and training all personnel responsible for employee access authorization and status change notification process. The entity completed the mitigation activities and FRCC verified completion.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007994	VAR-001-1	R6; R6.1	The entity self-reported an issue with VAR-001-1 R6.1. The entity identified six instances where a plant operator notified the energy control center generation system operator of a change in automatic voltage regulator (AVR) status. In each instance, the energy control center failed to give a voltage directive to the Generator Operator, as required by the Standard. In the first instance, the entity's plant operator informed the entity's energy control center that he needed to take the AVR to manual for approximately ten minutes in order to perform routine maintenance. The energy control center failed to provide the plant operator with a voltage directive. In the second instance, the entity's plant operator informed the entity's energy control center that he needed to take the AVR out of service for maintenance for approximately 40 minutes. In this instance, the energy control center operator failed to provide a voltage directive to the plant operator. In the third instance, the entity's plant operator informed the entity's energy control center that he needed to take the AVR out of service for maintenance for approximately one hour. In this instance, the energy control center operator failed to provide a voltage directive to the plant operator. In the fourth instance, the entity's plant operator informed the entity's energy control center that he needed to take the AVR out of service for maintenance for approximately 30 minutes. In this instance, the energy control center operator failed to provide a voltage directive to the plant operator. In the fifth instance, the entity's plant operator informed the entity's energy control center that he needed to place the AVR in manual mode for approximately eight hours. In this instance, the energy control center operator failed to provide a voltage directive to the plant operator. In the sixth instance, the entity's plant operator informed the entity's energy control center that he needed to place the AVR in manual mode for approximately 48 hours. In this instance, the energy control center operator failed to provide a voltage	FRCC determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system and only posed a minimal risk. The risk of the underlying issue is minimal because, in each instance, the Transmission Operator was aware of the unavailability of the AVR and was maintaining voltage manually. The TOP would have been able to notify the Reliability Coordinator quickly in case of any issue. In addition, the failure to give plant operators directives with respect to the AVR status occurred on units with output of less than 110 MW and 30 MVAR. FRCC considered the fact that the entity has violated this Standard previously. The prior violation occurred in 2009, two years prior to the issue at hand. Following the 2009 violation, the entity implemented AVR training, gave directives to energy control center supervisors regarding AVR status changes, and modified its Energy Management System (EMS) so generation system operators and transmission system operators receive an alarm from units that can automatically announce an AVR or Power System Stabilizer (PSS) status change. FRCC determined that FFT treatment is appropriate in this case because of the enhanced mitigation measures implemented by the entity and in particular the new and revised procedural controls and standing order, as well as the minimal level of risk of the underlying issues.	The entity completed the following mitigation activities: (1) continuing training was conducted and all involved energy control system operators participated; (2) new procedural control regarding AVR/PSS status change tracking was created; (3) a standing order was released; and (4) procedural control regarding AVR/PSS voltage schedules for generating plants was revised to incorporate the contents of the standing order.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007996	TOP-005-1.1a	R1	The entity self-reported an issue with TOP-005-1.1a R1. The entity identified two instances where a plant operator notified the energy control center generation system operator of a change in automatic voltage regulator (AVR) status and the energy control center failed to inform the Reliability Coordinator. It should be noted that the same system operator was on duty for both instances. In the first instance, the entity's plant operator informed the entity's energy control center that he needed to take the AVR to manual for approximately ten minutes in order to perform routine maintenance. The energy control center failed to report the change in status to the FRCC Reliability Coordinator (RC). The energy control center also failed to notify the RC once the plant operator reported the AVR back in automatic. In the second instance, the entity's plant operator informed the energy control center that he needed to take the AVR to manual for approximately thirty minutes in order to perform routine maintenance. The energy control center again failed to report the change in status to the RC and failed to notify the RC once the plant operator reported the AVR back in automatic.	FRCC determined that this issue did not pose a serious or substantial risk to the reliability of the bulk power system and only posed a minimal risk. The risk of the underlying issue is minimal because, in each instance, the Transmission Operator was aware of the unavailability of the AVR and was maintaining voltage manually. The Transmission Operator would have been able to notify the Reliability Coordinator quickly in case of any issue. In addition, the failure to give plant operators directives with respect to the AVR status occurred on units with output of less than 110 MW and 30 MVAR. FRCC considered the fact that the entity has violated this Standard previously. The prior violation occurred in 2009, two years prior to the issue at hand. Following the 2009 violation, the entity implemented AVR training, gave directives to energy control center supervisors regarding AVR status changes, and modified its Energy Management System (EMS) so generation system operators and transmission system operators receive an alarm from units that can automatically announce an AVR or Power System Stabilizer (PSS) status change. FRCC determined that FFT treatment is appropriate in this case because of the enhanced mitigation measures implemented by the entity and in particular the new and revised procedural controls and standing order, as well as the minimal level of risk of the underlying issues.	The entity completed the following mitigation activities: (1) continuing training was conducted and the involved energy control system operator participated; (2) new procedural control regarding AVR/PSS status change tracking was created; (3) a standing order was released; and (4) procedural control regarding AVR/PSS voltage schedules for generating plants was revised to incorporate the contents of the standing order.

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) Alexandria Light & Power (ALP)	NCRXXXXX	MRO201100369	CIP-003-1	R2	During a compliance audit, MRO determined that the entity had an issue with CIP-003-1 R2 for failing to assign a senior manager with overall responsibility for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because failure to assign a senior manager did not change the implementation of the entity's cyber security policy, or the senior manager overseeing the implementation of the policy. Although the entity lacked a formal documented assignment, the senior manager did sign the policy. Additionally, the entity is summer peaking with an all time peak of less than 100 MW in July 2007, and has less than 20 miles of transmission line.	The entity designated a senior manager with the authority and responsibility for leading and managing the implementation of CIP-002 through CIP-009 compliance. The entity completed its mitigation activities, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100302	CIP-007-1	R1	The entity self-reported an issue with CIP-007-1 R1 because it failed to document test results which indicate whether initial testing of new Cyber Assets within the Electronic Security Perimeter adversely affect existing cyber security controls, including a scan of open/enabled ports and services. Specifically, the entity did not have any documentation to verify the initial testing of the security configuration of the relay access devices, identified as Critical Cyber Assets (CCAs), at the substations to ensure no adverse effects to existing security controls.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because during the installation process, the devices were commissioned employing the same controls as other CCAs. Additionally, the devices were field-tested at the time of installation to confirm their standard configuration. The deficiency was in the absence of documentation of the baseline standard configuration test.	The entity conducted a scan of the relay access devices in which the baseline of required ports and services was compared to actual ports and services discovered during that scan. Also, further testing was performed to determine the necessary configuration changes. As a result, the required changes to CCAs to enable only required ports and services were defined, deployed and completed at all relevant locations
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3)	NCRXXXXX	MRO201100294	CIP-007-2	R3	The entity self-reported an issue with Reliability Standard CIP-007-2 R3 because it failed to document the assessment of security patches for applicability within thirty calendar days of availability of the patches. The entity conducted a search of the National Institute of Standards and Technology National Vulnerability Database (NIST NVD) for Common Vulnerabilities and Exposures (CVEs) to identify security patches or upgrades, but no results were returned for the particular identified software; however, there was a new security patch. The entity subsequently learned that the NIST NVD CVE summary application names were not identical to the vendor's application names registered on the Cyber Assets, and therefore did not identify the security patch in its search.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because in order to exploit the vulnerability, users have to access a malicious website. The Electronic Security Perimeter (ESP) access point protecting the Cyber Assets with this identified software prohibits users from accessing websites outside the ESP.	The entity performed the following actions to mitigate the issue: (1) assessed patches; (2) modified the manual NIST NVD search criteria; (3) expanded its configuration management system to include specific software; (4) developed and implemented an in-house NIST NVD search tool; and (5) updated the CIP security patch management job aid with detailed instructions for the new in-house NIST NVD search tool. The entity completed its mitigation activities, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4) Northern States Power (Xcel Energy) (NSP)	NCRXXXXX	MRO201000179	CIP-003-1	R4	During a CIP spot check, MRO determined that the entity had an issue with CIP-003-1 R4 for failing to label the entity's disaster recovery plans and Critical Asset lists according to the entity's energy information security classifications policy.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity has a document software package which facilitates secure content management and limits electronic access to authorized users. The documents not marked in accordance with the energy information security classifications policy were within a restricted area of the system. Only a limited number of authorized users were able to access the documents.	The entity performed the following actions to mitigate the issue: (1) conducted a comprehensive CIP review; and (2) marked the disaster recovery plans and Critical Asset lists documents in accordance with its energy information security classifications policy.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5) Willmar Municipal Utilities (WLMRWL)	NCRXXXXX	MRO201100388	CIP-001-1	R2	During a compliance audit, MRO discovered that the entity had an issue with CIP-001-1 R2 for failing to have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity does not have any Critical Assets, and it has not had any reportable sabotage events. Additionally, the entity owns less than 20 miles of transmission line and has a peak load of less than 100 MW.	The entity modified its sabotage reporting procedure to include instructions to communicate sabotage events to appropriate parties in the Interconnection. The entity completed its mitigation activities, as verified by MRO.

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	RFC201000405	COM-002-2	R2	Reliability*First* conducted a compliance audit of the entity. During the compliance audit, Reliability*First* determined that on five instances, the entity did not issue a directive to a third-party according to the requirements stated in COM-002-2 R2. Specifically, Reliability*First* determined that on four occasions, the entity issued directives which were not clear and concise, pursuant to COM-002-2 R2. On one occasion, Reliability*First* determined that the entity did not repeat back a directive or acknowledge the response as correct, pursuant to COM-002-2 R2.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). Reliability*First* determined that the five directives in question were related to VAR-001-1 R12 which requires the registered entity to "direct corrective action, including load reduction necessary to prevent voltage collapse when reactive resources are insufficient." Although Reliability*First* found that the directives did not meet the requirements of COM-002-2 R2, the entity was not found to have failed to direct corrective actions in the type of scenario contemplated in VAR-001 R12. Specifically, Reliability*First* found no instances of noncompliance with VAR-001-1 R12 as well as no issues related to insufficient amounts of reactive support. In addition, the entity is no longer registered on the NERC Compliance Registry as a Transmission Operator nor Balancing Authority, and is not subject to COM-002-2 R2. Moreover, the entity had a communication procedure in place during the time of the issue which required its employees to follow three-part communication when issuing directives regarding system reliability matters. As indicated in the description of the mitigation activities, these procedures and existing training were reinforced.	In its mitigation plan, the entity memorialized the actions it took to address the issue of COM-002-2 R2. The entity began including a reminder in all daily briefings for operations staff to emphasize clear and concise communications and always use three-part communications when issuing directives. The entity completed developing additional training for its operations staff focused solely on three-part communication. The entity also conducted monthly evaluations of randomly selected voice recordings in order to evaluate its compliance with COM-002-2 R2. The entity completed its mitigation plan, which Reliability*First* verified.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201000666	EOP-004-1	R3; R3.1	The entity submitted a Self-Report to Reliability*First* identifying a possible issue with EOP-004-1 R3.1. On a single day, the entity experienced a storm that resulted in loss of power to more than 50,000 customers for more than one hour. The entity submitted the preliminary written report (Preliminary Report) submitted to the U.S. Department of Energy (DOE) of the storm to Reliability*First* and NERC 88 hours after the 24-hour reporting period, as required by the Standard. Subsequently, as part of an internal extent-of-condition review, the entity identified another storm that had occurred two years before the first identified storm, which resulted in loss of power to more than 50,000 customers for more than one hour and for which the entity submitted the final DOE Report approximately two days late, and has no record that it submitted copies of the Preliminary Report to Reliability*First* or NERC.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Each of the reportable incidents were storm-related, and the entity submitted Preliminary Reports to the DOE within 48 hours for each of the reportable incidents. Additionally, for the first identified storm, the entity submitted the Preliminary Report to Reliability*First* and to NERC within four days. As part of the entity's mitigating actions, it also submitted the Preliminary Report to Reliability*First* and NERC for the storm that occurred 2 years previously. Reliability*First* became aware of the events when the entity submitted the Preliminary Report in one instance (approximately four days after the event), and the Final Report in another instance (approximately two days after the event).	The entity conducted training on its revised emergency procedures to promote awareness and reinforce the importance of EOP-004-1 to its employees. In addition, the entity revised its emergency notification procedures by identifying the responsible staff for submitting the Preliminary Report, adding DOE notification instructions, and clarifying the appropriate process for submission of the Preliminary Report and final DOE Report, clarifying the appropriate process for submission of the Preliminary Report and final DOE Report to include NERC, Regional Reliability Organization and Regional Transmission Organization submissions. The entity notified the relevant personnel of these revisions. Upon identifying the full extent of the issue, the entity developed a matrix for emergency notification procedures to assist personnel in quickly identifying appropriate responsibilities and tasks, and further revised and disseminated its emergency notification procedures to reflect these revisions.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2011001120	VAR-002-1.1b	R1	The entity submitted a Self-Report of a possible issue with VAR-002-1.1b R1 to Reliability*First*. The entity reported that on multiple occasions over a three-year period, it started three generating units in manual mode until the units reached minimum unit-stability-related output levels, as necessitated by the design of the equipment, at which point the units were switched to automatic voltage control mode. The entity also reported that during those occurrences it failed to notify its Transmission Operator of the manual voltage control mode status.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the foregoing facts and circumstances was mitigated by the following factors. The entity started the three generating units in manual mode due to the design of the equipment. The three generators, although identified as single generating units, are each actually comprised of two separate generators. At startup, the generators are operated in manual voltage control mode to minimize undesirable mechanical stress and variability of current on the generators. This also enables the entity to ensure that the generators are loaded equally and stabilized together. Once this occurs, the entity switches the generating units to automatic voltage control mode and releases them for dispatch. The entity only does so after the generating units have been stabilized and their respective voltage regulators have been set to automatic voltage control mode. The entity's procedure for manual mode startup, which was in place during the pendency of this issue, contributed to reducing the risk to the BPS by maintaining system stability.	The entity mitigated this issue by reviewing and reissuing standing orders related to VAR-002-1.1b R1, and updating the startup procedures for the affected units to include direct and explicit notifications to the Transmission Operator that a unit will be operating in manual mode during upcoming startup followed by an update that the unit has changed to automatic voltage control after reaching minimum unit-stability-related output levels. The entity completed mitigation activities for the issue.

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 4 (RFC_URE4)	NCRXXXXX	RFC201100989	FAC-008-1	R1	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered a possible issue of FAC-008-1 R1. The entity has a Facility Ratings Methodology in place; however, the entity included only relay settings for relay protective devices, which are not the Facility Ratings for those devices. Reliability*First* determined that the entity had an issue with the Standard as it failed to include all equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The wind generating facility is designed such that the wind turbine generators constitute the most limiting element. Although the entity failed to include a Facility Rating for its relay protective devices, the device that would limit the amount of generation remained the same. Therefore, when the entity revised its Facility Ratings to include relay protective devices, its most limiting element did not change. Failure to include a Facility Rating for relay protective devices did not limit the generation output of the entity's system. The relay protective devices were designed to safely withstand the amount of generation the entity's system is capable of producing.	In its mitigation plan, the entity memorialized the actions it took to address the issue of FAC-008-1 R1. The entity revised its Facility Rating Methodology to include an analysis of relay protective device Ratings analyzed against maximum steady state current flow and performed a new assessment of the entity's Facility using the revised Facility Ratings Methodology. The entity completed its mitigation activities, as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2011001053	FAC-008-1	R1	Reliability*First* conducted a compliance audit of the entity's corporate affiliate, during which Reliability*First* discovered a possible issue with FAC-008-1 R1 (RFC201100989). The findings from this compliance audit of the entity's affiliate led to additional self-certifications of issues with FAC-008-1 R1 by other corporate affiliates. The entity utilizes its affiliate's Facility Ratings Methodology, which the affiliate controls. The following month after the compliance audit, the entity self-certified an issue with FAC-008-1 R1. In its Facility Ratings Methodology, the entity's affiliate included only relay settings for relay protective devices which are not the Facility Ratings for those devices. Reliability*First* determined that the entity had an issue with the Standard as it utilized its affiliate's Facility Ratings Methodology, failing to include all equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The wind generating facility is designed such that the wind turbine generators constitute the most limiting element. Although the entity failed to include a Facility Rating for its relay protective devices, the device that would limit the amount of generation remained the same. Therefore, when the entity revised its Facility Ratings to include relay protective devices, its most limiting element did not change. Failure to include a Facility Rating for relay protective devices did not limit the generation output of the entity's system. The relay protective devices were designed to safely withstand the amount of generation the entity's system is capable of producing.	The entity's affiliate revised its Facility Ratings Methodology, which in turn revised the entity's Facility Ratings Methodology. The entity's affiliate completed its mitigation activities, which was verified by Reliability*First.*
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC2011001054	FAC-008-1	R1	The entity self-certified an issue with FAC-008-1 R1. A month earlier, Reliability*First* conducted a compliance audit of the entity's affiliate, during which Reliability*First* discovered a possible issue with FAC-008-1 R1 (RFC201100989). The findings from this compliance audit of the entity's affiliate led to additional self-certifications of FAC-008-1 R1 by other corporate affiliates. The entity utilizes its affiliate's Facility Ratings Methodology, which the affiliate controls. In its Facility Ratings Methodology, the entity's affiliate included only relay settings for relay protective devices, which are not the Facility Ratings for those devices. Reliability*First* determined that the entity had an issue with the Standard as it utilized its affiliate's Facility Ratings Methodology, failing to include all equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The wind generating facility is designed such that the wind turbine generators constitute the most limiting element. Although the entity failed to include a Facility Rating for its relay protective devices, the device that would limit the amount of generation remained the same. Therefore, when the entity revised its Facility Ratings to include relay protective devices, its most limiting element did not change. Failure to include a Facility Rating for relay protective devices did not limit the generation output of the entity's system. The relay protective devices were designed to safely withstand the amount of generation the entity's system is capable of producing.	The entity's affiliate revised its Facility Ratings Methodology, which in turn revised the entity's Facility Ratings Methodology. The entity's affiliate completed its mitigation activities, which was verified by Reliability*First.*
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC2011001055	FAC-008-1	R1	The entity self-certified an issue with FAC-008-1 R1. A month earlier, Reliability*First* conducted a compliance audit of the entity's affiliate, during which Reliability*First* discovered a possible issue of FAC-008-1 R1 (RFC201100989). The findings from this compliance audit of the entity's affiliate led to additional self-certifications of FAC-008-1 R1 by other corporate affiliates. The entity utilizes its affiliate's Facility Ratings Methodology, which the affiliate controls. In its Facility Ratings Methodology, the affiliate included only relay settings for relay protective devices, which are not the Facility Rating for those devices. Reliability*First* determined that the entity had an issue with the Standard as it, as it utilized its affiliate's Facility Ratings Methodology, failing to include all equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The wind generating facility is designed such that the wind turbine generators constitute the most limiting element. Although the entity failed to include a Facility Rating for its relay protective devices, the device that would limit the amount of generation remained the same. Therefore, when the entity revised its Facility Ratings to include relay protective devices, its most limiting element did not change. Failure to include a Facility Rating for relay protective devices did not limit the generation output of the entity's system. The relay protective devices were designed to safely withstand the amount of generation the entity's system is capable of producing.	The entity's affiliate revised its Facility Ratings Methodology, which in turn revised the entity's Facility Ratings Methodology. The entity's affiliate completed its mitigation activities, which was verified by Reliability*First* .

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 8 (RFC_URE8)	NCRXXXXX	RFC2011001052	FAC-008-1	R1	The entity self-certified an issue with FAC-008-1 R1. A month earlier, Reliability*First* conducted a compliance audit of the entity's affiliate, during which Reliability*First* discovered a possible issue of FAC-008-1 R1 (RFC201100989). The findings from this compliance audit of the entity's affiliate led to additional self-certifications of FAC-008-1 R1 by other corporate affiliates. The entity utilizes its affiliate's Facility Ratings Methodology, which the affiliate controls. In its Facility Ratings Methodology, the entity included only relay settings for relay protective devices, which are not the Facility Rating for those devices. Reliability*First* determined that the entity had an issue with the Standard, as it utilized its affiliate's Facility Ratings Methodology, failing to include all equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The wind generating facility is designed such that the wind turbine generators constitute the most limiting element. Although the entity failed to include a Facility Rating for its relay protective devices, the device that would limit the amount of generation remained the same. Therefore, when the entity revised its Facility Ratings to include relay protective devices, its most limiting element did not change. Failure to include a Facility Rating for relay protective devices did not limit the generation output of the entity's system. The relay protective devices were designed to safely withstand the amount of generation the entity's system is capable of producing.	The entity's affiliate revised its Facility Ratings Methodology, which in turn revised the entity's Facility Ratings Methodology. The entity's affiliate completed its mitigation activities, which was verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC201100855	CIP-008-2	R1	The entity submitted a Self-Report to Reliability*First* indicating that it had a possible issue with CIP-008-2 R1. The entity's Cyber Security Incident response plan (Response Plan) did not include a process for updating the Response Plan within 30 calendar days of any changes. Rather, the entity's Response Plan included a process for updating the Response Plan within 90 calendar days of any changes. Although Version 1 of CIP-008 allowed for a 90-day period to update the Response Plan, on April 1, 2010, Version 2 of CIP-008 took effect, which required registered entities to update their respective response plans within a shorter 30-day period. Therefore, from the effective date of CIP-008-2, the entity had an issue with CIP-008-2 R1.4.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that the issue is the result of a documentation error. It is a documentation error because although the entity's Response Plan stated that it must update the Response Plan within 90 days of any changes rather than within 30 days, the entity made no changes during the duration of the issue, and therefore, did not need to make any updates to the Response Plan.	In its mitigation plan, the entity outlined the actions it took to mitigate the issue. The entity revised its Response Plan to include a process for updating the Response Plan within 30 calendar days of any changes. The entity completed its mitigation activities, which was verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC201100856	CIP-006-2	R1; R1.4	The entity submitted a Self-Report to Reliability*First* indicating a possible issue CIP-006-2 R1. Specifically, the entity's physical security plan did not address response to loss and prohibition of inappropriate use of physical access controls pursuant to CIP-006-2 R1.4. The entity's training and corporate policies addressed response to loss and prohibition of inappropriate use, but those policies were not part of the physical security plan and were not approved by senior management, as required by CIP-006-2 R1.4. Additionally, the entity included a provision in its physical security plan which stated that the entity would update the physical security plan within 90 calendar days of the completion of any physical security system redesign or reconfiguration. Although Version 1 of CIP-006 R1.7 allowed for a 90-day period to update a physical security plan, on April 1, 2010, Version 2 of CIP-006 took effect, which required a shorter 30-day update period. Therefore, from the effective date of CIP-006-2, the entity did not include a requirement in its physical security plan to update the physical security plan within 30 days of a physical security system design or configuration change.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that the issue is the result of a documentation error. It is a documentation error because although the entity's physical security plan did not address response to loss or a prohibition of inappropriate use of physical access controls, the entity addressed these topics in corporate policies and trained its employees on these topics. Additionally, although the entity's physical security plan stated that it must update the physical security plan within 90 days of any changes rather than within 30 days, the entity made no changes during the duration of the issue, and therefore, did not need to make any updates.	In its mitigation plan, the entity outlined the actions it took to mitigate the issue. The entity revised its physical security plan to address response to loss and prohibition of inappropriate use of physical access controls. The entity also included a requirement to update the physical security plan within 30 days of a physical security system design or configuration change. The entity completed its mitigation activities, which was verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 10 (RFC_URE10)	NCRXXXXX	RFC2011001076	CIP-005-3	R1; R1.1	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered that the entity had a possible issue with the Standard. Reliability*First* discovered that the entity did not identify certain third-party vendor security device appliances as access points to Electronic Security Perimeters (ESPs). These appliances allow the third-party vendor to monitor activity on the entity's network and identify any unauthorized activities. These appliances are directly connected to mirrored ports on routers within the ESP. This issue involved nine of the entity's devices. The entity failed to identify these devices as access points to the ESP, as required by CIP-005-3 R1.1.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The entity included these appliances on its network diagrams, although it did not identify the appliances as access points to the ESP. The entity also afforded the same protections to the appliances as it provides to all access points to the ESP. Therefore, the entity merely failed to document the appliances as access points to the ESP and at all relevant times provided the requisite protections to the appliances. In addition, due to their being connected via mirrored ports, the appliances are only configured for monitoring traffic and for reporting anomalies out of the ESP. These appliances are not configured to carry information into the ESP. Furthermore, the appliances are located within Physical Security Perimeters.	In order to mitigate the issue, during the compliance audit, the entity, revised its network topology diagrams to identify the appliances as access points to the ESP. The entity completed its mitigation activities, which was verified by Reliability*First.*

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 11 (RFC_URE11)	NCRXXXXX	RFC2011001253	CIP-005-3	R1; R1.1	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered that the entity had a possible issue with the Standard. Reliability*First* determined that the facts and circumstances of an issue with the entity's affiliate also constituted a possible issue for the entity (RFC2011001076). Reliability*First* discovered that the entity did not identify certain third-party vendor security device appliances as access points to Electronic Security Perimeters (ESPs). These appliances allow the third-party vendor, to monitor activity on the entity's network and identify any unauthorized activities. These appliances are directly connected to mirrored ports on routers within the ESP. This issue involved nine of the entity's devices. The entity failed to identify these devices as access points to the ESP, as required by CIP-005-3 R1.1.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The entity included these appliances on its network diagrams, although it did not identify the appliances as access points to the ESP. The entity also afforded the same protections to the appliances as it provides to all access points to the ESP. Therefore, the entity merely failed to document the appliances as access points to the ESP and at all relevant times provided the requisite protections to the appliances. In addition, due to their being connected via mirrored ports, the appliances are only configured for monitoring traffic and for reporting anomalies out of the ESP. These appliances are not configured to carry information into the ESP. Furthermore, the appliances are located within Physical Security Perimeters.	In order to mitigate the issue, the entity, during the compliance audit, revised its network topology diagrams to identify the appliances as access points to the ESP. The entity completed its mitigation activities, which was verified by Reliability*First*.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 12 (RFC_URE12)	NCRXXXXX	RFC201100930	CIP-004-3	R3	The entity submitted a Self-Report for CIP-004-3 R3 to Reliability*First*. A month earlier, the entity's NERC compliance team notified the entity's security services team that they identified an unexpected individual on the daily physical access report. Upon further investigation, the entity discovered that it granted physical access to Critical Cyber Assets to the wrong individual. Specifically, a contractor performing fire alarm system work requested and was granted, access to the entity's headquarters building, which contains four Physical Security Perimeters (PSPs); however, the entity erroneously granted the access to the four PSPs to another contractor with another company, a credit union employee whose office is located in a different city. The other contractor did not have a background check on file, and therefore did not receive a personnel risk assessment as required by CIP-004-3 R3. The erroneous grant of access to the other contractor resulted from two issues in the entity's access request process. First, an entity employee failed to issue a user identification for the other contractor while creating the other contractor's employee record, which resulted in a null value for the other contractor in the employee database. Second, the access request submitted for the correct contractor was corrupted and did not have user identification, which also resulted in a null value for the correct contractor in the employee database. Since the null values matched, the system granted the correct contractor's access request to the other contractor.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the BPS posed by the foregoing facts and circumstances was mitigated by the following factors. The entity's daily physical access reports quickly pinpointed the erroneous grant of access to the other contractor, and as a result, the issue lasted less than one day. Additionally, the other contractor was unaware that the entity granted her access to the headquarters facility, and she did not attempt to use this access during the time period of the issue. Moreover, the other contractor worked in a separate physical facility in a different city from the location of the CCAs. Of the four PSPs to which the entity granted the other contractor access, two of the PSPs would have been inaccessible as a result of biometric security features installed in those PSPs. Additionally, the remaining two PSPs are small rooms in the entity's headquarters and would be difficult for an unauthorized individual to find and access.	In its mitigation plan, the entity memorialized the actions it took to address the issue of CIP-004-3 R3. The entity removed the access rights from the other contractor, reminded the other contractor's company of the proper data entry standards, and checked for additional null entries in the employee records database. The entity also updated its database forms to enforce proper data entry for the user identification field, and worked with its software vendor to implement similar error checking in its security badge management product. The entity completed its mitigation activities, which was verified by Reliability*First*.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 13 (RFC_URE13)	NCRXXXXX	RFC2011001242	CIP-007-3	R5.3	The entity submitted a Self-Report to Reliability*First*, identifying an issue with CIP-007-3 R5. The entity implemented a process to automate monitoring and alerts related to password age in order to improve its prior manual password review process. During this process, the entity discovered two local accounts on two of its servers within the Electronic Security Perimeter (ESP) with passwords that had not been changed annually. The entity had not changed the passwords on the accounts since their creation. Reliability*First* determined that the entity had an issue with CIP-007-3 R5 by failing to annually change the password on two of its local accounts.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Although located within the ESP, the two servers were not Critical Cyber Assets. The entity's other utility utilized the servers for historic data archiving, and the servers were logically isolated from the Energy Management System servers. Therefore, the servers at issue were not configured to affect BPS elements. In addition, the entity verified that the local accounts have never been accessed since their creation. Only a small group of information technology individuals with CIP cybersecurity training and current background checks had access to the local accounts. The local accounts were only accessible inside the ESP, for which the requisite protections were in place.	In order to mitigate the issue the entity deleted the two local accounts at issue. The entity completed its mitigation activities as verified by Reliability*First*.

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 14 (RFC_URE14)	NCRXXXXX	RFC2011001056	VAR-002-1.1b	R1	The entity submitted a Self-Report to Reliability*First* identifying an issue of VAR-002-1.1b R3.1. Subsequently, Reliability*First* determined that the facts of the issue of VAR-002-1.1b R3.1 also constituted an issue of VAR-002-1.1b R1. On a single day, the entity started the automatic voltage regulator (AVR) on one of its generating units in manual mode but failed to notify the Transmission Operator (TOP) that it would be operating the AVR in manual mode prior to operating the AVR in manual mode, as required by VAR-002-1.1b R1.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The entity's operating personnel placed the AVR into service as soon as practicable. The entity initially placed the AVR into manual mode pursuant to its operating procedures. The power plant maintained its voltage schedule at all relevant times. Furthermore, this constituted an isolated event corrected through personnel training.	The entity performed the following mitigating actions to address the issue of VAR-002-1.1b R1. The entity entered into a memorandum of understanding with its TOP which provided the TOP with a standing notification of the entity's startup and shutdown procedures. The standing notification provides details regarding when, pursuant to applicable procedures, each of the entity's generating units' AVRs will be operating outside of automatic mode, and when they will switch back into automatic mode. Therefore, the entity has notified its TOP of (a) its operation of certain of its AVRs outside of automatic mode during startup and shutdown procedures, and (b) the status change on certain AVRs during startup and shutdown procedures. The entity completed its mitigation activities as verified by Reliability*First*.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 14 (RFC_URE14)	NCRXXXXX	RFC201100939	VAR-002-1.1b	R3; R3.1	The entity submitted a Self-Report to Reliability*First* identifying an issue of VAR-002-1.1b R3.1. Local operating personnel at the entity's power plant placed the automatic voltage regulator (AVR) into service as soon as practicable but the entity failed to notify the Transmission Operator (TOP) of this status change within 30 minutes of the status change, as required by VAR-002-1.1b R3.1.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The entity provided notification to the TOP within nine minutes of operating the AVR in manual mode. Therefore, despite failing to notify the TOP prior to operating the AVR in manual mode, the entity did so almost immediately afterward.	In its mitigation plan, the entity memorialized the actions it took to address this issue. The entity reviewed the applicable requirement with the control room operator on shift during the time of the issue. In addition, the entity verified that the AVR placard informing personnel of requirements was in place. Furthermore, the entity met with power plant operating personnel to discuss Reliability Standard requirements, including AVR notification requirements.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 15 (RFC_URE15)	NCRXXXXX	RFC2011001228	CIP-006-3c	R1	Reliability*First* determined, during a compliance audit, that the entity had an issue with CIP-006-3c R1. The entity failed to maintain a six-wall border around the control room of one of its facilities, which contains Critical Cyber Assets. Specifically, a 12-inch gap exists between the tops of the walls and the ceiling. Reliability*First* determined that the entity had an issue with CIP-006-3c R1 by failing to maintain a six-wall border around all Cyber Assets within an Electronic Security Perimeter (ESP). The entity filed a late Technical Feasibility Exception (TFE) request with Reliability*First* stating that the operational limitations of its heating, ventilation, and air conditioning system required the 12-inch gap, and modifications could affect air circulation in the facility.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. The entity used motion sensors to monitor the 12-inch gap in the six-wall border and this mitigating measure has been fully implemented and approved by Reliability*First*. The facility in question is also secured by security fencing and a guarded single access gate. Additionally, both the building that contains the main control center and the control center itself restrict access via card-reader equipment with monitoring and alarming features. All compensating measures were in place for the duration of the issue.	Reliability*First* accepted and approved the entity's late TFE request.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 15 (RFC_URE15)	NCRXXXXX	RFC2011001233	CIP-007-3	R4	Reliability*First* found, during a compliance audit, that the entity had an issue with CIP-007-3 R4. Reliability*First* determined that the entity had an issue with CIP-007-3 R4 by failing to use anti-virus software and other malware prevention tools on all Cyber Assets within the Electronic Security Perimeter. The entity submitted two late Technical Feasibility Exception (TFE) requests related to Cyber Assets for which there were no available malware prevention tools. Specifically, the entity stated that both affected devices run proprietary operating systems for which no manufacturer or third-party malware prevention tools exist. The entity filed the two TFE requests with Reliability*First*. Reliability*First* accepted the TFE requests and approved them on.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors, which the entity provided as compensating measures for the TFEs. Both Cyber Assets run on proprietary operating systems on which malware development is unlikely. The Cyber Assets are located behind firewalls that restrict traffic, and remote access to them requires two-factor authentication. The entity also protects the Cyber Assets with video surveillance. These compensating measures were in place for the duration of the issue.	Reliability*First* accepted and approved the entity's two late TFE request.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 15 (RFC_URE15)	NCRXXXXX	RFC2011001238	CIP-008-3	R1.6	Reliability*First* found, during a compliance audit, that the entity had an issue with CIP-008-3 R1.6. Although the entity was able to provide a Cyber Security Incident response plan (Plan), it failed to include within the Plan a process for ensuring that it was tested at least annually. Although it failed to have a documented process within the Plan, the entity was able to provide evidence that it did test the Plan annually. Reliability*First* determined that the entity had an issue with CIP-008-3 R1 by failing to include within its Plan a process for ensuring that the Plan is tested at least annually.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk posed to BPS was mitigated by the fact that the issue was a documentation error because although the entity did not document a process within the Plan to ensure that it tests the Plan annually, the entity did test the Plan annually.	The entity provided evidence that it updated its Plan to include a process for annual testing as required by CIP-008-3 R1.6. The entity completed its mitigation activities as verified by Reliability*First*.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCRXXXXX	SPP201000301	CIP-003-1	R1; R1.1	SPP RE discovered an issue with CIP-003-1 R1.1 during a spot check. The entity's Cyber Security Policy (CSP), during the period which entity was required to comply with CIP-003-1 R1, failed to address all of the requirements of CIP-002-1 through CIP-009-1, as required by CIP-003-1 R1.1. On the date on which version two of the CIP standards went into effect, the entity enacted a new CSP, which addressed all of the requirements of CIP-002-2 through CIP-009-2, as required by CIP-003-2 R1.1. SPP RE determined that the entity's CSP under CIP version one failed to address the following: CIP-004-1 R2.1, R2.1; CIP-005-1 R1.5, R2.1, R2.6; CIP-006-1 R1.1 through R1.7; CIP-007-1 R1.1, R1.2, R4.2, R5.2.2, R5.2.3, R5.3.2; CIP-008-1 R1.1, R1.4.	SPP RE determined that 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 entity had a CSP in place and on the date version two of the CIP standards went into effect, and prior to the spot check, entity enacted a new CSP that addressed the requirements of CIP-003-2 R1. Although the entity's prior CSP for CIP did not address every requirement, it did address each of the main level requirements of all of the CIP standards. In paraphrasing the requirements of CIP-002 through CIP-009, the entity omitted some of the included requirements. The CSP, however, still served the purpose of conveying management's commitment and ability to secure the entity's Critical Cyber Assets.	The entity, prior to the spot check, had implemented a new CSP in order to comply with version two of the CIP standards. The entity certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000343	BAL-005-0.1b	R8	The entity submitted a Self-Report stating that during internal evaluations of compliance with this requirement it was discovered that a limited number of Remote Terminal Unit (RTU) scan rates at locations with data acquisition inputs into the Area Control Error (ACE) equation were not being scanned at least every six seconds as required by the Standard. Rather the RTUs had a longer scan rate. The SPP RE reviewed the entity's Self-Report and accompanying evidence and determined that there was a reasonable basis for an issue related to this Standard.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1) a limited number of RTUs had scan rates greater than six seconds; 2) the scan rate for these RTUs was longer than the required six seconds; and 3) the longer scan rate did not introduce a noticeable error in the entity's ACE calculation. The entity did not experience any disturbances or impact to reliability as a consequence of the locations having a longer second scan rate. Further, the entity's system was continuing to calculate ACE values for the entity's Balancing Authority every two seconds to insure proper automatic generator control performance.	To mitigate its issue with BAL-005-0.1b R8, the entity changed its RTU scan rates at the identified locations. In addition, the entity created a procedure that provided that all data acquisition for and calculation of ACE occurred at least every six seconds. The entity certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000432	BAL-003-0.1b	R2; R2.1	During an SPP RE compliance audit of the entity, SPP RE's audit team discovered an issue of NERC Reliability Standard BAL-003-0.1b R2.1. SPP RE's audit team discovered that the entity, in determining its fixed Frequency Bias, failed to establish its fixed Frequency Bias by observing and averaging the Frequency Response for several disturbances. Instead of observing and averaging "several" disturbances, the entity used the most severe disturbance to determine its fixed Frequency Bias.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not use "several" disturbances to determine its fixed Frequency Bias, the disturbances it used were the most severe disturbances, resulting in a fixed Frequency Bias that was equal to or greater than the Frequency Bias it otherwise would have determined by averaging the frequency response for several disturbances. Because the entity's fixed Frequency Bias was equal to or greater than its average Frequency Response, SPP RE has determined that the issue posed a minimal risk to the BPS. Additionally, the entity used several disturbances to calculate its current Frequency Bias.	The entity revised its procedure and will continue to follow the methodology it used to determine its Frequency Bias, which addresses the requirement of this Standard, to ensure that several disturbances are, and will be, analyzed when establishing the bias setting. The entity certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000433	EOP-005-1	R1	During a compliance audit, the SPP RE audit team discovered that the entity had an issue with EOP-005-1 R1 because the entity did not have evidence that several system operators received System Restoration training as required by Attachment 1 to EOP-005-1 (Elements for Consideration in Development of Restoration Plans) Element # 7, which states that documentation must be retained in the personnel training records that operating personnel have been trained annually in the implementation of the plan and have participated in restoration exercises. After further review, the entity determined that it did not have evidence that several system operators received System Restoration training, as required by this Standard.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had evidence that the system operators had performed multiple system restoration training simulations in the past and following the issue period. Therefore, each of the system operators had participated in training and were familiar with system restoration.	To mitigate its issue with EOP-005-1 R1, the entity added the annual requirement for system operator training on restoration procedures to its applicable training plans. The entity certified that mitigation was complete, and SPP RE verified completion.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000434	EOP-008-0	R1; R1.6	During a compliance audit, SPP RE's audit team identified an issue with EOP-008-0 R1.6 because the entity's Loss of Control Center Functionality plans did not document the responsibility for the annual training on the plans as required in R1.6. The entity had two Loss of Control Center Functionality plans. The entity's procedure stated that operator training and drill using this procedure will be conducted at least annually by each system operator. While the procedures required that training be performed, the procedure did not contain specific language addressing who had the responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plans, as required by this Standard.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: (1) annual training and drills were being conducted throughout the duration of this issue; (2) the entity's plans otherwise met the requirements of EOP-008-0 R1, were well developed and provided comprehensive checklists for the system operators to follow; and (3) the entity promptly mitigated the issue by updating its procedures.	To mitigate this issue, the entity updated its plans to include specific responsibility for annual training. The entity certified that that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000435	FAC-001-0	R2 (R2.1.4, R2.1.6 through R2.1.11)	During a compliance audit, the SPP RE audit team discovered that the entity's policy did not provide a written summary adequately addressing the following sub-requirements, as required by this Standard: R2.1.4. Breaker duty and surge protection R2.1.6. Metering and telecommunications. R2.1.7. Grounding and safety issues. R2.1.8. Insulation and insulation coordination. R2.1.9. Voltage, Reactive Power, and power factor control. R2.1.10. Power quality impacts. R2.1.11. Equipment Ratings.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity's issue was documentation related. Although the entity's policy did not adequately address all of FAC-001-0 R2.1's sub-requirements (R2.1.4, R2.1.6 through R2.1.11), the entity was addressing these requirements in the course of approving a facility connection. The entity demonstrated its performance by providing an agreement which sufficiently addressed the sub-requirements of R2.1 missing in the entity's policy.	To mitigate its issue with FAC-001-0, the entity modified its policy to incorporate requirements found in other process documents and procedures that address R2.1.4, R2.1.6 through R2.1.11 sub-requirements of FAC-001-0 R2.1. The entity certified that that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000436	FAC-008-1	R1; R1.2.1	During a compliance audit of the entity, the SPP RE audit team identified an issue with FAC-008-1 R1 because the entity's Facility Rating Methodology did not adequately provide a method for rating the individual equipment making up the facility, *i.e.* , generators, transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices, as required by this Standard.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity had not documented a methodology for rating the individual equipment comprising its generation facilities, it had determined the rating of its generation facilities by performing a capacity test in accordance with the procedures established in Southwest Power Pool's Criteria. Accordingly, there was not a material difference between the generation facility capacity determined before and after mitigation of the this issue. The entity's capacity tests on its generating units provided an accurate capacity rating for planning purposes.	To mitigate this issue with FAC-008-1 R1.2.1, the entity replaced its Generation Methodology with a new procedure. The procedure incorporated facility ratings methodology for generators, generator iso-phase bus conductor, and generator step up (GSU) transformers. Also, the procedure addressed the ratings methodology for the following: 1. Conductors 2. Transformers 3. Disconnect Switches 4. Generator Breakers 5. Protective Relay Devices 6. Terminal Equipment 7. Series and Shunt Compensation Devices; and 8. Rigid Bus The entity approved its procedure and certified that mitigation was complete. SPP RE verified completion.

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 1 (WECC_URE1)	NCRXXXXX	WECC2011008711	CIP-007-2	R4	WECC_URE1 submitted two late-filed Technical Feasibility Exceptions (TFEs) addressing infeasibility with CIP-007-2 R4 for firewalls. The entity stated that the devices are incapable of running anti-malware software on its firewall appliance in its supported configuration.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the devices associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. The entity has implemented a two-factor authentication for external interactive access, also any firmware (memory location) change on the device requires a reboot for the device to take effect. A network intrusion detection system (NIDS) monitors for threats on the local area network within the Electronic Security Perimeter(s), any security events from the device and NIDS are logged to a central security event monitoring console. Further, the Physical Security Perimeter and restricted access to only authorized personnel deters local misuse and introduction of malware.	Entity filed the TFEs, WECC approved the Part A and Part B TFE. The vendor hardened the cyber asset. A separate security monitoring appliance is used to detect anomalous behavior on the network.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2011008712	CIP-005-3	R2	WECC_URE1 submitted one late-filed Technical Feasibility Exception (TFE) addressing infeasibility with CIP-005-3 R2 for an electronic access control system. The entity stated the device does not support the display of an appropriate use banner prior to an interactive access attempt (login and password prompt) for a system administrator account on the device.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the device associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. The entity stated the appropriate use banner is displayed after successful entry of a valid user ID, PIN and two factor authentication key for system administrative access to the device. Further, security events from the device and the network intrusion detection system are logged.	Entity filed the TFEs, WECC approved the Part A and Part B TFE. Two factor authentication is implemented for remote interactive access through the firewalls. A Physical Security Perimeter was implemented.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2011008713	CIP-007-1	R4	WECC_URE2 submitted one late-filed Technical Feasibility Exception (TFE) addressing infeasibility with CIP-007-1 R4 for a control system. The entity stated that anti-virus software was installed on the device which resulted in failure of the device after a couple of days. Upon further investigation, it was discovered that the server failed due to a memory leak from a communication protocol system process. Although the memory leak already existed prior to the antivirus being installed, the support staff believed the anti-virus software exasperated the issue based on continuous scanning of the system. The entity has since uninstalled the anti-virus software.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the device associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. The entity stated that the device is on a local area network only with internet connectivity, the device's secure configuration disables/removes software such as email clients that could make the server vulnerable to a virus. Further, the device is within a Physical Security Perimeter(s) and Electronic Security Perimeter(s).	Entity filed the TFEs, WECC approved the Part A and Part B TFE. Compensating measures were applied to limit exposure, such as no direct Internet connections or e-mail accounts are allowed on the system, and disabling of the auto run/auto play feature was performed. Anti-malware will be evaluated for compatibility if it becomes available.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2011008714	CIP-007-1	R6	WECC_URE3 submitted one late-filed Technical Feasibility Exception (TFE) addressing infeasibility with CIP-007-1 R6 for peripheral devices (*e.g.* printers). The entity stated that these devices are incapable of employing security access monitoring.	WECC determined that this issue posed a minimal risk and a not serious or substantial risk to the reliability of the bulk power system (BPS). WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the devices associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. The entity implemented all available security measures supported by the device (*e.g.* strong passwords and disabling of used ports and services). Neighboring networked devices that do employ all security features are fully monitored for usual activity to provide visibility and will provide periphery notification in the event that the device begins exhibiting unusual or suspicious behavior. Further, strong Physical Security Perimeter(s) boundaries are enforced to reduce the risk of a physical compromise to the device.	Entity filed the TFEs, WECC approved the Part A and Part B TFE. All available security measures supported by the devices are implemented. Neighboring networked devices that do employ all security features are fully monitored for unusual activity to provide visibility.

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	WECC2011008715	CIP-005-2	R2	WECC_URE4 submitted two late-filed Technical Feasibility Exceptions (TFEs) addressing infeasibility with CIP-005-2 R2 for an electronic access control system. The entity stated that client application used for administration of devices does not support the deployment of appropriate use banners on all of its interfaces. The web user and the command line interfaces only allow configuration changes to be made to the firewalls and do not provide full administration capabilities of the firewall, including changes to firewall access control lists.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the devices associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. To compensate for the lack of an acceptable use banner, WECC_URE4 has placed these two instances of the application behind two factor authentication (which contains the appropriate use banner) to restrict and control access. Access has been further restricted by limiting permitted network connections to a small number of dedicated IP address reservations which are locked to the individual firewall administrators' domain accounts. Additionally, all firewall administrators have undergone background checks, and administrators must first acknowledge an acceptable use banner on their workstation computers before they are able to instantiate and operate any instance of the software. Further, accounts on the application are limited to the minimum privilege level necessary to administer the systems. WECC_URE4 has also implemented strong passwords for all administrative accounts to minimize the possibility of unauthorized access. The strong passwords meet WECC_URE4 and CIP complexity requirements, and are changed at least annually. Procedures are also in place to ensure passwords are changed should any of the administrators leave WECC_URE4 or no longer have responsibility for the devices.	Entity filed the TFEs, WECC approved the Part A and Part B TFE. Access to the application was restricted using two factor authentication (which contains appropriate use banner) and network connections were limited to dedicated IP addresses locked to individual domain accounts of firewall and VPN administrators exceeding CIP access standards.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900043	CIP-002-1	R1	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. NCEA also found that: (i) One third party entity had a risk-based assessment methodology that was flawed in that it was not reliability-based, but instead had business criteria considered in the calculations to determine the Critical Asset (CA) List. The entity still had substations and control centers on its CA List. (ii) Another third party entity eliminated assets from consideration for the CA List based upon setting risk at various levels less than unity. The methodology had a primary control center declared as a "high criticality asset" initially but it was eliminated by setting the vulnerability and likelihood of compromise at significantly less than unity.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900044	CIP-002-1	R2	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. NCEA also found that one third party entity's policy had insufficient references to the requirements in Standards CIP-002 through CIP-009 related to emergency situations. Another third party entity did not provide evidence that its policy was available to all personnel who have access to, or are responsible for, Critical Cyber Assets.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900045	CIP-002-1	R3	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. NERC found that third party entities failed to provide information or did not provide information sufficient to indicate that they met the requirement as of July 1, 2008. Furthermore NERC found that third party entities failed to provide information or did not provide information sufficient to indicate that they met the requirement at the time of their spot check.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900049	CIP-004-1	R2	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, two third party entities did not provide evidence that their security training program was reviewed annually or that it was updated as necessary.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900050	CIP-004-1	R3	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, two third party entities provided no evidence that personnel risk assessments (PRAs) had been conducted for all employees, contractors, and service vendor personnel with authorized cyber access or unescorted physical access; the evidence provided by two third party entities did not indicate that PRAs were updated every 7 years and/or for cause; four third party entities provided no evidence of PRA results.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900051	CIP-004-1	R4	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. After all evidence was reviewed, it was discovered that for one third party entity, no evidence was provided listing employees with authorized cyber access and/or unescorted physical access. For four third party entities, no evidence was provided listing contractors and service vendors with authorized cyber access and/or unescorted physical access. For three third party entities, there was no evidence that access list(s) are reviewed quarterly. For three third party entities, there was no evidence that access list(s) are updated within 7 days of any change in access rights. For two third party entities, there was no evidence that access list(s) for contractors and service vendors were properly maintained. For two third party entities, there was no evidence that access was revoked within 24 hours for personnel terminated for cause. Finally, for three third party entities, there was no evidence that access was revoked within 7 calendar days for personnel who no longer required access.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue. .	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900052	CIP-007-1	R1	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, for one third party entity, several requirements listed in the standard were not included in the documentation provided.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900053	CIP-008-1	R1	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, one third party entity did not address several requirements listed in the standard; another third party entity's evidence did not indicate what procedures were used to characterize and classify events as reportable Cyber Security Incidents; yet another third party entity's evidence did not indicate a process for ensuring that its Cyber Security Incident response plan was tested at least annually.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900054	CIP-009-1	R1	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, one third party entity's evidence did not adequately support compliance with the standard; another third party entity's recovery plan did not fully specify the appropriate actions for responding to situations of varying duration and severity.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900055	CIP-009-1	R2	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, one third party entity's evidence did not clearly indicate how the sample test report pertains to the recovery of Critical Cyber Assets (CCAs) and another third party entity's test evidence for failover did not specifically address CCA recovery, as is necessary per the standard purpose statement, so they did not have a valid annual exercise.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900040	PER-003-0	R1	The entity did not ensure that third party entities that were performing tasks on its behalf met the requirements of this standard. NCEA found that: (i) one third party entity did not staff all operating positions, with the primary responsibility for the real-time operation of the interconnected BES, with NERC-certified personnel. That third party entity's subject matter expert (SME) stated that non-certified operators, responsible for real-time operation/switching, performed transmission switching without direct oversight/direction from a NERC-certified operator. (ii) None of a second third party entity's operators were NERC-certified. Its SME stated that the entity had eight operators and three assistants. Its operators, responsible for real-time operation/switching, were performing transmission switching without direct oversight/direction from a NERC-certified operator. (iii) Yet another third party entity did not staff all operating positions, with the primary responsibility for the real-time operation of the interconnected BES, with NERC-certified personnel. Its SME stated that non-certified operators, responsible for real-time operation/switching, performed transmission switching without direct oversight/direction from a NERC-certified operator. (iv) Finally, another third party entity did not have a NERC-certified operator on duty at all times with the result that non-certified operators, responsible for real-time operation, performed transmission switching without direct oversight/direction from a NERC-certified operator.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system because NCEA considered that: (i) The noncompliance of three of the four third party entities arose because they did not staff all relevant operating positions with NERC-certified operators at all times. The source and degree to which each was non-compliant is as follows: (a) 18 of one third party entity's 21 operators were NERC-certified. (b) Another third party entity clarified that all of its dispatchers were either NERC-certified or in the process, through a formal, defined 5-year program, towards certification. Furthermore: all planned facility outages were first reviewed and approved by NERC-certified personnel before they could be executed. Operators not yet certified could conduct switching under proper supervision of a NERC-certified operator as stipulated in its certification program dependent upon the non-certified operator's current certification progression level. Finally, at least one NERC-certified dispatcher was in the operations center at all times. (c) The third entity required its system operators to obtain NERC certification in due course. All operators, including NERC-certified, were required to participate in on the job system operator training and continuing education, and were allowed to do switching upon demonstration of the required competencies. (d) The last third party entity is a municipal electric department serving a municipality of less than 100,000 people. The municipality's 2009 annual reports indicate that it provided 64,000 to 65,000 MWh of energy per month to 37,000 to 38,000 accounts in 2008 and 2009.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900042	PER-002-0	R3.1	The entity did not ensure that third party entities that were performing tasks on its behalf met the requirements of this standard. A third party entity did not provide evidence that its training program had defined objectives based on entity operating procedures. Rather, it provided evidence that it uses a vendor for training objectives based on NERC Standards. It was unable to present objectives for entity operating procedures.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system because NCEA considered that the third party entity did not comply with the standard and could not rely on the efforts by another third party entity who was not separately subject to the standard. The third party entity's training program was found to lack the objectives required by PER-002-0 R3, but a subsequent spot check of the third party entity found no evidence of noncompliance based on evidence reviewed with respect to PER-003-0.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900041	EOP-008-0	R1.5	The entity did not ensure that third party entities that were performing tasks on its behalf met the requirements of this standard. Specifically, a third party entity did not conduct annual tests at its control center to ensure the viability of its contingency plan. It stated this during its interview with the audit team. It provided evidence that tests were conducted in 2005, 2006 and 2009. Therefore, tests of the plan were not conducted in the 2007 and 2008 calendar years.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system because NCEA considered that, over the period of the issue, only 2 tests were missed which resulted in a limited scope and limited impact of the issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900046	CIP-003-1	R1	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, a third party entity's evidence did not demonstrate the policy was available to all employees who had access to CCAs and another third party entity's policy had insufficient references to the requirements in Standards CIP-002 through CIP-009 related to emergency situations.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900047	CIP-003-1	R2	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, a third party entity's evidence did not show that it had developed a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA200900048	CIP-003-1	R3	The entity did not include in its methodology or assessment the CIP assets of other third party entities that were performing tasks on its behalf. Due to different compliance schedules, there was a gap in timing for compliance with respect to those assets. Specifically, a third party entity's evidence did not demonstrate it used a list of Critical Assets developed pursuant to R2, nor that it developed a list of associated Critical Cyber Assets essential to the operation of the Critical Asset.	This issue posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS) because NCEA considered that, over the period of the issue, the third party entities were preparing for compliance with the CIP standards, as required by the Approved Implementation Plan. There was no actual impact to reliability of the BPS as a result of the subject issue.	Coordinated Functional Registration agreements were put in place to address respective responsibilities. The methodologies and assessments were corrected and the respective third party entities were certified for the applicable function and had to demonstrate compliance at that time with this requirement.

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR JANUARY 2012 FIND FIX AND TRACK REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

Sarah Rogers*
President and Chief Executive officer
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
srogers@frcc.com

Linda Campbell*
VP and Executive Director Standards & Compliance
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
lcampbell@frcc.com

Barry Pagel*
Director of Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 690
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5648 – facsimile
bpagel@frcc.com

FOR MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Director of Regulatory Affairs and Enforcement
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1708
se.patrick@midwestreliability.org

FOR RFC:

Robert K. Wargo*
Director of Enforcement and Regulatory Affairs
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
bob.wargo@rfirst.org

L. Jason Blake*
Corporate Counsel
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
jason.blake@rfirst.org

Megan E. Gambrel*
Associate Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
megan.gambrel@rfirst.org

Michael D. Austin*
Associate Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
mike.austin@rfirst.org

FOR SPP RE:

Stacy Dochoda*
General Manager
Southwest Power Pool Regional Entity
16101 La Grande, Ste 103
Little Rock, AR 72223
(501) 688-1730
(501) 821-8726 – facsimile
sdochoda.re@spp.org

Joe Gertsch*
Manager of Enforcement
Southwest Power Pool Regional Entity
16101 La Grande, Ste 103
Little Rock, AR 72223
(501) 688-1672
(501) 821-8726 – facsimile
jgertsch.re@spp.org

Machelle Smith*
Paralegal & SPP RE File Clerk
Southwest Power Pool Regional Entity
16101 La Grande, Ste 103
Little Rock, AR 72223
(501) 688-1681
(501) 821-8726 – facsimile
spprefileclerk@spp.org

FOR WECC:

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

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6855
(801) 883-6894 – facsimile
CWhite@wecc.biz

Sandy Mooy*
Associate General Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7658
(801) 883-6894 – facsimile
SMooy@wecc.biz

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

FOR NCEA:

Sean Bodkin*
Compliance Enforcement Coordinator
North American Electric Reliability Corporation
1325 G Street NW, Suite 600
Washington, DC 20005
(202) 400-3000
sean.bodkin@nerc.net

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RC12-___-000

NOTICE OF FILING
January 31, 2012

Take notice that on January 31, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty (30) Registered Entities in five (5) Regional Entity footprints and NERC as the Compliance Enforcement Authority.

Any person desiring to intervene or to protest this filing must file in accordance with Rules 211 and 214 of the Commission's Rules of Practice and Procedure (18 CFR 385.211, 385.214). Protests will be considered by the Commission in determining the appropriate action to be taken, but will not serve to make protestants parties to the proceeding. Any person wishing to become a party must file a notice of intervention or motion to intervene, as appropriate. Such notices, motions, or protests must be filed on or before the comment date. On or before the comment date, it is not necessary to serve motions to intervene or protests on persons other than the Applicant.

The Commission encourages electronic submission of protests and interventions in lieu of paper using the "eFiling" link at http://www.ferc.gov. Persons unable to file electronically should submit an original and 14 copies of the protest or intervention to the Federal Energy Regulatory Commission, 888 First Street, N.E., Washington, D.C. 20426.

This filing is accessible on-line at http://www.ferc.gov, using the "eLibrary" link and is available for review in the Commission's Public Reference Room in Washington, D.C. There is an "eSubscription" link on the web site that enables subscribers to receive email notification when a document is added to a subscribed docket(s). For assistance with any FERC Online service, please email FERCOnlineSupport@ferc.gov, or call (866) 208-3676 (toll free). For TTY, call (202) 502-8659.

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Document Accession #: 20120201-5137 Filed Date: 02/01/2012

Document Content(s)