Federal Energy Regulatory Commission
Washington, D.C. 20426

January 31, 2022

FOIA No. FY19-30 (RC12-2)
Fifty Seventh Determination
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated January 25, 2022, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC12-2, along with the names of five (5) relevant UREs inserted, 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 RC12-2

With respect to the remaining identities of UREs contained in RC12-2, 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

[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.

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-2 will not be disclosed.

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

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

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2022.01.31 14:39:10 -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 #: 20111130-5278 Filed Date: 11/30/2011

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC12-2

MidAmerican Energy Company (MEC)-.pdf page 20

Tatanka Wind Power, LLC (TWP)-.pdf page 21-22

Lakewood Cogeneration, LP (Lakewood)-.pdf page 25

NAEA Ocean Peaking Power, LLC (OPP)-.pdf page 25

City of Bentonville, Arkansas (Bentonville)-.pdf page 29

November 30, 2011

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 50 possible violations[5] of 17 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 50 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 1120 G Street N.W., Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile 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 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile 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
1120 G Street N.W., Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net

cc: Entities listed in Attachment B

NERC

Attachment a

Fix and Track Report Spreadsheet (Included in a Separate Document)

NERC

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR NOVEMBER 2011 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 NPCC:

Walter Cintron*
Manager, Compliance Enforcement
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas – 10th Floor
New York, New York 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
wcintron@npcc.org

Edward A. Schwerdt*
President and Chief Executive Officer
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
eschwerdt@npcc.org

Stanley E. Kopman*
Assistant Vice President of Compliance
Northeast Power Coordinating Council, Inc.
1040 Avenue of the Americas, 10th Floor
New York, NY 10018-3703
(212) 840-1070
(212) 302-2782 – facsimile
skopman@npcc.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 SERC:

R. Scott Henry*
President and CEO
SERC Reliability Corporation
2815 Coliseum Centre Drive
Charlotte, NC 28217
(704) 940-8202
(704) 357-7914 – facsimile
shenry@serc1.org

Marisa A. Sifontes*
General Counsel
Maggie Sallah*
Legal Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7775
(704) 357-7914 – facsimile
msifontes@serc1.org
msallah@serc1.org

Kenneth B. Keels, Jr.*
Director of Compliance
Andrea Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive
Charlotte, NC 28217
(704) 940-8214
(704) 357-7914 – facsimile
kkeels@serc1.org
akoch@serc1.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 Texas RE:

Susan Vincent*
General Counsel
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4922
(512) 233-2233 – facsimile
susan.vincent@texasre.org

Rashida Caraway*
Manager, Compliance Enforcement
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4977
(512) 233-2233 – facsimile
rashida.caraway@texasre.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

NERC

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
November 30, 2011

Take notice that on November 30, 2011, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty (30) Registered Entities in eight (8) Regional Entity footprints.

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

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100422	TOP-004-2	R1	The entity submitted a Self-Report regarding an issue with TOP-004-2 R1. Specifically, it did not operate within the Interconnection Reliability Operating Limits (IROLs) and System Operating Limits (SOLs). During the one-day event, a failed static wire resulted in the outage of two 138 kV transmission lines. These outages led to what appeared to be MVA limit conditions on a 230/138 kV autotransformer.	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 outage of the two 138 kV circuits, led to indicated MVA limit conditions on the 230/138 kV autotransformer; however, even if the transformer had tripped, the result would have been loss of local entity internal load. There would not be any instability, uncontrolled separation, or cascading outages resulting from the loss of the 230/138 kV autotransformer because the transformer would have only affected loss of local entity internal load. Also, although there was an indicated overload on the autotransformer, due primarily to cold weather, the autotransformer was never actually overloaded. This was confirmed by subsequent review of industry standards, dissolved gas analysis and electrical testing of the autotransformer which showed the transformer was actually under rated.	The entity mitigated the issue by performing the following activities: (1) The entity enhanced its Facility Rating Methodology to include Rating flexibility to account for cold weather conditions and the specific characteristics of autotransformers and other power system equipment. A new Methodology was developed by entity operations to include normal and emergency winter Ratings. This new Methodology complies with all Reliability Standards; (2) The entity also updated its operations procedures to include actions to take in cold weather conditions as it relates to the enhanced Rating Methodology. System operations procedures were updated to include specific list of actions to take in anticipation of and during cold weather conditions. The procedures include a process for utilizing winter Ratings. The procedures also include a process where the system operator can review and modify as appropriate, specific emergency limits based on real-time information; (3) Furthermore, the entity provided training to operators, which included a review of the following: (a) the event in detail; (b) its new Rating Methodology with operators, especially cold weather normal and emergency Ratings; (c) the modified operations procedures; (d) appropriate standards, responsibilities and expectations of transmission operators for SOLs and other equipment overloads, with emphasis on cold weather operations; and (e) remedial action plans with emphasis on actions during cold weather operations. The entity completed its mitigation plan, as verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC2011007254	CIP-006-3c	R1	During a spot check, FRCC determined that the entity is subject to the Standard. On two separate occasions, when a visitor was granted access to the Physical Security Perimeter (PSP), the entity failed to document that name of the personnel responsible for providing continuous escorting to the visitor as required by its visitor control program for visitors procedure (R1.6).	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the concerned PSP is manned 24 hours a day and seven days a week and on the two instances of the issue the operator did escort the visitor but failed to document the logs.	This issue has been mitigated by the entity by documenting the logs and the mitigation plan includes additional milestones to prevent recurrence by revising its visitor control program for visitors procedure documentation and providing training to all staff responsible for escorting visitors. The entity completed its mitigation plan, as verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007691	FAC-009-1	R1	The entity was found during a spot check that it did not consider its transmission conductors, jumpers, and aluminum bus when it established Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology. The transmission equipment excluded is limited to approximately 225 feet of 230 kV radial line which connects the entity to its Balancing Authority's (BA) substation. The remaining section of the radial line is owned by the BA.	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 was operating its equipment within manufacturer and design specifications. Moreover, the entity is located at one power plant site with a single radial 230 kV line connecting it to its BA.	The entity hired a consultant to provide recommended changes to the entity's list of equipment including transmission conductors, jumpers and aluminum bus, the required Ratings, and the supporting documentation for the Ratings. The consultant also evaluated the equipment relative to the most limiting applicable Equipment Rating and, if necessary, made recommendations concerning the most limiting Equipment Rating. All of these recommendations were provided to the entity in a written report. The entity revised its FAC-008 and FAC-009 procedures to reflect the Facility Ratings changes. The entity completed its mitigation plan, as verified by FRCC.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100262	CIP-009-1	R4	During a Spot Check, MRO discovered that the entity failed to provide backup records of network switches which are classified as Critical Cyber Assets (CCAs) for the previous full calendar year in its recovery plan for CCAs. Due to the “First In First Out” (FIFO) storage method utilized by the entity's backup system, previous switch configurations are “rolled off” after a certain number of new configuration versions are backed up. Furthermore, the entity’s backup solution only retains the data for 90 days once it has been removed from the actual server. While the entity could demonstrate that its backup system was performing its intended function throughout the time period covered by the Spot Check, the system’s design could not produce evidence that a backup was performed on a specific date and time.	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 all of the appropriate backups of information required to successfully restore the entity's CCAs were being performed, even though documentation was found to be inadequate.	The entity established and documented a process to record and retain documentation demonstrating the successful archival of network switches data backup. To confirm the backup is being performed as required the system automatically issues a change control ticket when the backup is completed. The ticket is assigned to a member of the network team who will verify the archival process was successful. The entity completed its mitigation plan, as verified by MRO.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201000167	PRC-005-1	R1; R1.1; R1.2	The entity self-reported noncompliance with PRC-005-1 R1.1 and R1.2 as its transmission Protection System maintenance and testing program failed to include a basis for maintenance and testing intervals for voltage and current sensing devices, station batteries and DC control circuitry, and also failed to include a summary of its maintenance and testing procedures.	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 performed the maintenance and testing for 93.5% of its Protection System devices within its defined maintenance and testing intervals. Additionally, the entity generates and transmits power to 13 rural electric cooperatives and associations and had an annual peak of less than 600 MW in 2009. The entity solely owns or jointly owns the equivalent of less than 100 miles of 115 kV, less than 250 miles of 161 kV, and less than 100 miles of 345 kV circuits. All 345 kV circuit miles are jointly owned generator outlet facilities.	The entity performed the following actions to mitigate the remediated issue: (1) revised its transmission Protection System maintenance and testing program document to include all elements of the Protection System, addressing BPS equipment identification, summarizing maintenance and testing procedures, and specifying maintenance and testing intervals with their basis; and (2) created a reference document to describe how maintenance and testing is performed in the integrated transmission system. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201000168	PRC-005-1	R2; R2.1; R2.2	The entity self-reported noncompliance with PRC-005-1 R2.1 because it failed to maintain and test its transmission Protection System devices in accordance with the defined intervals in its Protection System maintenance and testing program. Upon receiving the Self-Report, MRO requested a full inventory of the entity's Protection System maintenance and testing records. The entity reported that it has 861 Protection System devices subject to the Standard. The entity failed to maintain and test 56 devices out of 861 total devices, or approximately 6.5%. Specifically, the entity failed to test 7 protective relays, 7 station batteries and 42 DC control circuits in accordance with its transmission Protection System maintenance and testing program.	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's relays within the scope of this remediated issue were being continuously monitored via its supervisory control and data acquisition system. Additionally, the entity generates and transmits power to 13 rural electric cooperatives and associations and had an annual peak of less than 600 MW in 2009. The entity solely owns or jointly owns the equivalent of less than 100 miles of 115 kV, less than 250 miles of 161 kV, and less than 100 miles of 345 kV circuits. All 345 kV circuit miles are jointly owned generator outlet facilities.	The entity performed the following actions to mitigate the issue: (1) performed a complete inventory of each BPS device and identified all deficiencies; (2) developed a "catch-up" maintenance and testing plan and schedule in order to correct any deficiency; (3) trained its technicians regarding revisions to the transmission Protection System maintenance and testing program; (4) trained its technicians regarding catch-up testing; (5) notified contractor personnel regarding revisions to the entity's BPS Protection System maintenance and testing program; (6) notified contractor personnel in the catch-up maintenance and testing procedures; and (7) completed the required catch-up maintenance and testing procedures. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3) MidAmerican Energy Company (MEC)	NCRXXXXX	MRO201100251	CIP-006-1	R1; R1.1	During a CIP Spot Check, conducted between August 16, 2010 through August 26, 2010, MRO determined that the entity, as a Responsible Entity registered as a Balancing Authority, Generator Operator, Generator Owner, Load-Serving Entity, Transmission Operator and Transmission Owner, failed to have a completely enclosed Physical Security Perimeter (PSP) with a completely enclosed ("six-wall") border as part of its physical security plan. The extent of the undefined border was at least the length of the door and about 1.5 feet in depth. The entity mitigated the PSP gap during the Spot Check and MRO reviewed and verified the mitigating measures.	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 multiple layers of security would need to be penetrated before gaining access to the PSPs. One of the PSPs is manned 24 hours per day, seven days per week. Both facilities contain Cyber Assets that have strong electronic protective measures in place. Specifically, at one PSP, there are at least ten security control types, including combinations of card readers, bio readers, mantrap, door status switches, human observer, proprietary keys, high security fence, padlocks, cameras and anti-tailgating devices. All paths have at least four security layers and at least three different types of security controls within those layers. At the other PSP, there are at least five security control types, including combinations of card readers, mantraps, door status switches, human observer and proprietary keys. All paths have at least four security layers to infiltrate before gaining access to the PSPs.	The entity performed the following to mitigate the remediated issue: (1) placed heavy wire mesh over the opening; (2) replaced the flexible ducts with rigid duct work; (3) developed a guide document for its staff to assist with the identification of "six-wall" borders and access points. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201000200	CIP-004-1	R2; R2.1; R2.3	During a CIP Spot Check, MRO determined that the entity had established, documented and maintained an annual cyber security training (CST) program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs); however, the entity's documentation was not sufficient to demonstrate that all personnel having authorized cyber or authorized unescorted physical access to CCAs had completed the training. Although the entity maintains that the training was provided prior to granting access to those individuals, who were provided paper copies of the training, the entity's records did not clearly identify that those individuals had received the training within ninety calendar days of such authorization (R2.1) and conducted at least annually, including the date the training was completed and attendance records (R2.3).	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 this was a documentation deficiency where the entity's process did not clearly identify the individuals receiving the training. The entity provided annual training to all personnel with authorized cyber or authorized unescorted physical access to CCAs in 2010 and again in 2011.	The entity performed the following actions to mitigate the remediated issue: (1) updated its CIP personnel system to automatically read computer based testing results and track the completion date; (2) updated the CIP personnel system to automatically send an email out to employees and their supervisors when retraining is required; (3) retrained all employees with security access via the computer-based training (CBT) method; (4) retrained and proctored all contractors with access to CCAs; and (5) updated its CIP-004 R2 corporate document with the new training processes for employees and contractors. The entity completed its mitigation plan, as verified by MRO.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201000201	CIP-004-1	R3	During a CIP Spot Check, MRO determined that the entity had an incomplete personnel risk assessment for one employee and could not corroborate statements that personnel risk assessments had been conducted within thirty days of such personnel being granted authorized cyber or authorized unescorted physical access to Critical Cyber Assets and updated at least every seven years or for cause, pursuant to the program required in R3 for three contractors. The entity had relied upon unverified attestations from the contractors.	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 although only a partial record was available, the personnel risk assessment for the employee had been completed. The entity conducted a new personnel risk assessment for the employee and found no issues with it. Additionally, the entity verified the personnel risk assessments for the three contractors and found no issues with them.	The entity performed the following actions to mitigate the remediated issue: (1) updated personnel risk assessments from 2004 and 2005 to address the seven-year criminal background issue and provide a list of employees with access and associated background check dates; (2) updated its contract language to assure that background check requirements meeting the relevant CIP standards for contractors and vendors are clearly set forth in the contract; (3) audited all personnel risk assessment records for contractors and provided a list of contractors with unescorted access and dates of completed and verified background check dates; and (4) updated its CIP-004 R3 corporate document with the background check verification processes for employees and contractors. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201000202	CIP-004-1	R4; R4.1; R4.2	During a CIP Spot Check, MRO determined that although the entity maintains a list of individuals with physical and cyber access to Critical Cyber Assets (CCAs) via its CIP personnel program, the entity failed to demonstrate that it had a process in place to be notified by its vendors when an individual has been terminated by the vendor, either with or without cause and update and maintain the access list accordingly within seven calendar days of any personnel change as required by CIP-004-1 R4.1. As a result, access was not revoked for three contractors who no longer required access within seven calendar days as required by CIP-004-1 R4.2.	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 none of the contractors had any access to the entity's facilities after they were terminated. In addition, none of the contractors had electronic access to the entity's CCAs. In addition, the failure of the vendor to report the employees' dismissal did not account for any security-related events.	The entity performed the following actions to mitigate the remediated issue: (1) the criminal background screening requirements section of the entity's contract service agreement was revised to include provisions for notifying the entity when unescorted access is no longer required or contractor's employee is terminated for cause; (2) CIP corporate annual training was updated with access removal requirements for employees and contractors and vendors and all employees and contractors and vendors were retrained to receive the updated training; and (3) contractors and vendors and their entity sponsors will be notified of the requirements for authorized unescorted access removal on a semi-annual basis. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5) Tatanka Wind Power, LLC (TWP)	NCRXXXXX	MRO201100327	CIP-001-1	R1	The entity self-certified noncompliance with CIP-001-1 R1 because it did not have procedures for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection. The entity failed to have such procedures for a 29-month period.	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 own any Critical Cyber Assets. Additionally, the entity's total generation is rated at less than 200 MVA.	The entity developed an official sabotage reporting procedure for Reliability Standard CIP-001-1 and trained personnel on the procedure. The procedure included: (1) recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection; (2) communicating of information concerning sabotage events to appropriate parties in the Interconnection; (3) providing its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events; and (4) reporting as appropriate to circumstances to the established local Federal Bureau of Investigation communications contacts. The entity completed its mitigation plan, as verified by MRO.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5) Tatanka Wind Power, LLC (TWP)	NCRXXXXX	MRO201100328	CIP-001-1	R2	The entity self-certified noncompliance with CIP-001-1 R2 because it did not have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. The entity failed to have such procedures for a 29-month period.	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 own any Critical Cyber Assets. Additionally, the entity's total generation is rated at less than 200 MVA.	The entity developed an official sabotage reporting procedure for Reliability Standard CIP-001-1 and trained personnel on the procedure. The procedure included: (1) recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection; (2) communicating of information concerning sabotage events to appropriate parties in the Interconnection; (3) providing its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events; and (4) reporting as appropriate to circumstances to the established local Federal Bureau of Investigation communications contacts. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5) Tatanka Wind Power, LLC (TWP)	NCRXXXXX	MRO201100329	CIP-001-1	R3	The entity self-certified noncompliance with CIP-001-1 R3 because it did not provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events. The entity failed to have such procedures for a 29-month period.	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 own any Critical Cyber Assets. Additionally, the entity's total generation is rated at less than 200 MVA.	The entity developed an official sabotage reporting procedure for Reliability Standard CIP-001-1 and trained personnel on the procedure. The procedure included: (1) recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection; (2) communicating of information concerning sabotage events to appropriate parties in the Interconnection; (3) providing its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events; and (4) reporting as appropriate to circumstances to the established local Federal Bureau of Investigation communications contacts. The entity completed its mitigation plan, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5) Tatanka Wind Power, LLC (TWP)	NCRXXXXX	MRO201100330	CIP-001-1	R4	The entity self-certified noncompliance with CIP-001-1 R4 because it did not establish contacts with the local Federal Bureau of Investigation (FBI) and develop reporting procedures as appropriate to its circumstances. The entity failed to have such procedures for a 29-month period.	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 own any Critical Cyber Assets. Additionally, the entity's total generation is rated at less than 200 MVA.	The entity developed an official sabotage reporting procedure for Reliability Standard CIP-001-1 and trained personnel on the procedure. The procedure included: (1) recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection; (2) communicating of information concerning sabotage events to appropriate parties in the Interconnection; (3) providing its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events; and (4) reporting as appropriate to circumstances to the established local FBI communications contacts. The entity completed its mitigation plan, as verified by MRO.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007273	CIP-007-1	R4	The entity self-reported non-compliance with CIP-007-1 R4 stemming from the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The TFE was requested because malware and anti-virus software cannot be installed on several assets. There were 15 late TFE requests of which 14 were filed 45 days late. The TFE Part A approval for all was granted by NPCC 4 days later.	NPCC determined that there was a minimal risk to the reliability of the bulk power system, and the issue did not pose a serious or substantial risk. The entity's system is structured with intrusion prevention sensors at the network and host level, hardened operating systems, strong account management, logging for system configuration changes, and periodic vulnerability scans which are run on the devices in question. These compensating measures were in place well before the past due date for TFE request submittals to NPCC.	The TFE Part A approval was granted by NPCC. The approved TFE requests are open-ended because the hardened operating system in question does not support third party software.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007276	CIP-004-1	R2; R2.1	After reviewing a Self-Report submitted by the entity for a possible violation of CIP-007-1 R4, NPCC, in its investigation, determined that the entity was noncompliant with CIP-004-1 R2 because personnel having access to Critical Cyber Assets (CCAs), including contractors and service vendors, were not trained prior to the CIP Implementation Table date on the entity's annual cyber security training program. The entity discovered that three employees continued to have physical access to CCAs for a time after the compliance enforcement date without having completed cyber security training. At the time of the Self-Report, the cyber security training had already been completed for the three employees. The duration of physical access past the compliance enforcement date without having completed the cyber security training was 101 days, 105 days and 111 days for the three employees.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no intentional or unintentional actions committed by any of the three employees as a result of not completing cyber security training before having physical access granted. There was minimal potential impact because the employees accessed areas that were staffed 24 hours a day, seven days a week. These areas were also monitored by cameras while access to those areas was logged.	1. The entity provided NPCC with various documents and spreadsheets showing that it had performed a full review of all PRA, cyber training and access list records going back to the compliance enforcement date. 2. The entity provided NPCC with revised policies associated with termination of employment and the protection of critical energy infrastructure and information. 3. The entity provided NPCC with documentation that the revised policies and future expectations had been shared with the relevant business units. The mitigation activities were completed as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007277	CIP-004-1	R3	After reviewing a Self-Report submitted by the entity for a possible violation of CIP-007-1 R4, NPCC, in its investigation, determined that the entity was noncompliant with CIP-004-1 R3 because a personnel risk assessment (PRA) was not conducted prior to the CIP Implementation Table date for personnel that had already been granted access to Critical Cyber Assets. The entity discovered that two employees continued to have physical access to CCA for a time after the compliance enforcement date without a completed PRA. At the time of the Self-Report, the PRA had already been completed for the two employees. The two employees continued to have physical access to Critical Cyber Assets after the compliance enforcement date for differing durations (8 months and 7.75 months) until the required PRAs were completed.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no intentional or unintentional actions committed by the two identified employees as a result of a PRA not being completed before having physical access granted. There was minimal potential impact because both employees accessed areas that were staffed 24 hours a day, seven days a week and monitored by cameras and access to those areas was logged.	1. The entity provided NPCC with various documents and spreadsheets showing that it had performed a full review of all PRA, cyber training and access list records going back to the compliance enforcement date. 2. The entity provided NPCC with revised policies associated with termination of employment and the protection of critical energy infrastructure and information. 3. The entity provided NPCC with documentation that the revised policies and future expectations had been shared with the relevant business units. The mitigation activities were completed as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007278	CIP-004-1	R4; R4.1; R4.2	The entity self-reported noncompliance with CIP-004-1 R4. The entity discovered that reviews of Physical Security Perimeter/Electronic Security Perimeter (PSP/ESP) access rights list did not occur in such fashion after the compliance enforcement date to ensure that revocation of access rights were completed as per R4.1. The entity is a CIP Implementation Table 4 entity with a 12/5/09 due date for becoming compliant. The entity did not review the list(s) of its personnel who have access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel, nor ensure access list(s) for contractors and service vendors were properly maintained. As a result of not reviewing access rights within a regular fashion after the compliance enforcement date, three instances were found that exceeded the 7-day revocation limit for personnel who no longer require such access to CCAs as per R4.2. The duration of the three instances were 2 days, 27 days and 14 months.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no access attempts made by the employees after the date that rights were no longer needed. There was minimal potential impact related to the first identified employee as the entity was only 2 days late revoking access. There was minimal potential impact related to the second identified employee. Although SCADA access for this employee still existed, he would have had to have an escort into the control room (his physical access had already been revoked) and remain there unsupervised to log onto an operating console. There was minimal potential impact related to the third identified employee because physical access rights were revoked in 2008 and would have required an escort into the entity's facilities before gaining access to use the unrevoked Windows administrative rights.	1. The entity provided NPCC with various documents and spreadsheets showing that it had performed a full review of all PRA, cyber training and access list records going back to the compliance enforcement date. 2. The entity provided NPCC with revised policies associated with termination of employment and the protection of critical energy infrastructure and information. 3. The entity provided NPCC with documentation that the revised policies and future expectations had been shared with the relevant business units. The mitigation activities were completed as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011007730	CIP-004-1	R4; R4.1	The entity self-reported non-compliance with CIP-004-1 R4. The entity, in correspondence with its service company affiliate IT compliance office, discovered that Critical Cyber Asset access lists associated with privileged users in the affiliate IT group were reviewed on an annual basis instead of a quarterly basis as required by R4.1. The affiliate's IT group documents the approved access to the server, Human Machine Interface (HMI) PCs, and network switches. The duration of this issue is 21 months which concluded with the verified end date of mitigation activities.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no intentional or unintentional actions committed by the privileged users in the affiliate IT group due to the lack of quarterly access review. There was minimal potential impact because system logs are generated on a continual basis and reviewed every 90 days. Such log review includes validation of users who accessed or attempted access to the server, HMI PCs and network switches. In addition, user access can only be granted via an IT request form and is rescinded upon termination or change of duties. The HMI PCs require physical access to be used. Each PC is located within a defined PSP which requires authorized unescorted PSP access which is reviewed on a monthly basis.	1. The entity provided documentation that the IT compliance office was established. 2. The entity provided documentation from the responsible managers that the quarterly access review process had been documented and was completed for first quarter of the year for the server, the HMI PCs, and the network switches. The mitigation activities were completed as verified by NPCC.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011007728	CIP-004-1	R4; R4.1	The entity self-reported non-compliance with CIP-004-1 R4. The entity, in correspondence with its service company affiliate IT compliance office, discovered that Critical Cyber Asset access lists associated with privileged users in the affiliate IT group were reviewed on an annual basis instead of a quarterly basis as required by R4.1. The affiliate's IT group documents the approved access to the server and network switches. The duration of this issue is 15 months which concluded with the verified end date of mitigation activities.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no intentional or unintentional actions committed by the privileged users in the affiliate IT group due to the lack of quarterly access review. There was minimal potential impact because system logs are generated on a continual basis and reviewed every 90 days. Such log review includes validation of users who accessed or attempted access to the server and network switches. In addition, user access can only be granted access via an IT request form which is rescinded upon termination or change of duties.	1. The entity provided documentation that the IT compliance office was established. 2. The entity provided documentation from the responsible managers that the quarterly access review process had been documented and was completed for first quarter of the year for the server and the network switches. The mitigation activities were completed as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011007729	CIP-004-1	R4; R4.1	The entity self-reported non-compliance with CIP-004-1 R4. The entity, in correspondence with its service company affiliate IT compliance office, discovered that Critical Cyber Asset access lists associated with privileged users in the affiliate IT group were reviewed on an annual basis instead of a quarterly basis as required by R4.1. The affiliate's IT group documents the approved access to the server and network switches. The duration of this issue is 15 months which concluded with the verified end date of mitigation activities.	NPCC determined that there was a minimal risk to the reliability of the bulk power system (BPS), and the issue did not pose a serious or substantial risk. There was no actual impact to the BPS as there were no intentional or unintentional actions committed by the privileged users in the affiliate IT group due to the lack of quarterly access review. There was minimal potential impact because system logs are generated on a continual basis and reviewed every 90 days. Such log review includes validation of users who accessed or attempted access to the server and network switches. In addition, user access can only be granted access via an IT request form which is rescinded upon termination or change of duties.	1. The entity provided documentation that the IT compliance office was established. 2. The entity provided documentation from the responsible managers that the quarterly access review process had been documented and was completed for first quarter of the year for the server and the network switches. The mitigation activities were completed as verified by NPCC.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100782	PRC-004-1	R3	The entity is subject to compliance with PRC-004-1 R3. The entity submitted a Self-Report to Reliability*First* identifying an issue with PRC-004-1 R3. Reliability*First* developed a procedure pursuant to PRC-003 R1 that requires registered entities to report Misoperations that occur between January 1 and June 30, by August 31. The entity experienced a Misoperation where a relay operated when it should not have because its set point was lower than it should have been. Pursuant to Reliability*First*'s procedures, the entity was required to provide documentation of its Misoperation analysis and Corrective Action Plan to Reliability*First* by August 31. The entity completed all analysis and remedial actions regarding the Misoperation five days later; however, due to an improper data query in its reporting spreadsheet, the entity failed to submit its Misoperation analysis and Corrective Action Plan to Reliability*First* until six months past the due date. Reliability*First* determined that the entity had an issue with PRC-004-1 R3 by failing to provide documentation of its Misoperation analysis and Corrective Action Plan according to the Regional Reliability Organization's procedures developed for PRC-003 R1.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the following factors. The entity completed its Misoperation analysis and its Corrective Action Plan five days after the Misoperation. The issue occurred because an improper data query in the entity's reporting spreadsheet left out the Misoperation from the report to Reliability*First*. As a result, the risk that the entity would not analyze or correct the cause of its Misoperation was mitigated.	The entity performed the following mitigating activities. The entity provided its Misoperation analysis and Corrective Action Plan to Reliability*First*. The entity modified its operations database to produce Misoperation lists grouped by each calendar quarter to ensure that it records the Misoperations in the correct reporting period and to improve the review process of each relay operation. The revised process will accomplish the following: (1) indicate if the operation occurred on the BPS, (2) make the default designation "Misoperation" to ensure review, (3) add an interruption number and specific details of the operation, and (4) show the date when the Misoperation Committee reviewed the information. The entity completed mitigation activities for this issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001000	CIP-007-3	R4	The entity is subject to compliance with CIP-007-3 R4. The entity submitted a Self-Report to Reliability*First* identifying an issue with CIP-007-3 R4. The entity did not use anti-virus software and other malware prevention software for eight Critical Cyber Assets (CCAs), as required by CIP-007-3 R4. The entity believed the eight CCAs were integrated components of the servers on which they reside and, therefore, did not require separate anti-virus software or other malware prevention tools; however, six of these CCAs were self-contained modules within the server that provide a separate network connection for personnel to remotely manage the server under emergency conditions. The remaining two CCAs run directly on server hardware without requiring an additional underlying operating system. These characteristics of the eight CCAs necessitated that they have anti-virus software and other malware prevention tools. According to the entity, these eight CCAs were incapable of using anti-virus software and other malware prevention tools but the entity did not request a Technical Feasibility Exception (TFE) from Reliability*First* for the eight CCAs. Reliability*First* determined the entity failed to use anti-virus software and other malware prevention tools pursuant to CIP-007-3 R4 and did not submit TFE requests until 13 months after the compliance enforcement date.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the entity had compensating measures in place to meet the intent of CIP-007 R4 prior to the mandatory compliance date. Specifically, the entity installed firewalls at the perimeter of the Electronic Security Perimeter with an intrusion prevention system that can detect and prevent many types of malware from propagating. The entity also installed virus protection on workstations and servers as well as firewall software on its workstations. Passwords for the CCAs are stored securely in a server password database that is restricted to authorized personnel only. Finally, administrative access to the CCAs is limited to a small group of support personnel to further minimize risk exposure.	The entity mitigated the issue by submitting TFE requests concerning the eight Critical Cyber Assets (CCAs) at issue to Reliability*First,* which were subsequently accepted and approved by Reliability*First*. The entity completed mitigation activities for the issue.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3) Lakewood Cogeneration, LP (Lakewood)	NCRXXXXX	RFC201100937	CIP-002-2	R1; R1.1	The entity is subject to compliance with CIP-002-2 R1. The entity self-reported an issue with CIP-002-2 R1.1 to Reliability*First.* The entity determined it did not include evaluation criteria in its risk-based methodology (RBAM). The entity's evaluation criteria included engineering studies and discussions with subject matter experts. The entity made references in its RBAM to engineering study procedures, but did not include the actual evaluation criteria in its RBAM. Reliability*First* determined that the entity failed to include evaluation criteria in its RBAM, pursuant to CIP-002-2 R1.1.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the issue was administrative in nature. It was administrative because although the entity failed to document its evaluation criteria in its RBAM, it did evaluate all its assets according to engineering studies and discussions with subject matter experts. Further, the entity did not identify any new facilities or change the designation of previously identified facilities from Critical Assets after it included the evaluation criteria required by CIP-002-2 R1.1 in its RBAM.	The entity performed the following mitigating activities. The entity documented the evaluation criteria in its RBAM pursuant to CIP-002-2 R1.1. The entity also notified all personnel involved in managing and using the RBAM of the updates. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 4 (RFC_URE4) NAEA Ocean Peaking Power, LLC (OPP)	NCRXXXXX	RFC201100938	CIP-002-2	R1; R1.1	The entity is subject to compliance with CIP-002-2 R1. The entity self-reported an issue with CIP-002-2 R1 to Reliability*First*. The entity determined that it did not include evaluation criteria in its risk-based methodology (RBAM). The entity's evaluation criteria included engineering studies and discussions with subject matter experts. The entity made references in its RBAM to engineering study procedures, but did not include the actual evaluation criteria in its RBAM. Reliability*First* determined that the entity failed to include evaluation criteria in its RBAM pursuant to CIP-002-2 R1.1.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the issue was administrative in nature. It was administrative because although the entity failed to document its evaluation criteria in its RBAM, it did evaluate all its assets according to engineering studies and discussions with subject matter experts. Further, the entity did not identify any new facilities or change the designation of previously identified facilities from Critical Assets after it included the evaluation criteria required by CIP-002-2 R1.1 in its RBAM.	The entity performed the following mitigating activities. The entity documented the evaluation criteria in its RBAM pursuant to CIP-002-2 R1.1. The entity also notified all personnel involved in managing and using the RBAM of the updates. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100910	CIP-002-2	R1	The entity is subject to compliance with CIP-002-2 R1. The entity self-certified non-compliance with CIP-002-2 R1 to Reliability*First*. The entity determined it did not include evaluation criteria in its risk-based methodology (RBAM). The entity's evaluation criteria included engineering studies and discussions with subject matter experts. The entity made references in its RBAM to engineering study procedures, but did not include the actual evaluation criteria in its RBAM. Reliability*First* determined that the entity failed to include evaluation criteria in its RBAM pursuant to CIP-002-2 R1.1.	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), and did not pose a serious or substantial risk. 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 the entity did evaluate all its assets according to engineering studies and discussions with subject matter experts, but failed to document this evaluation. Further, the entity did not identify any new facilities or change the designation of previously identified facilities from Critical Assets after it included the evaluation criteria required by CIP-002-2 R1.1 in its RBAM.	The entity performed the following mitigating activities. The entity documented the evaluation criteria in its RBAM pursuant to CIP-002-2 R1.1. The entity also notified all personnel involved in managing and using the RBAM of the updates. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100911	CIP-003-2	R5	The entity is subject to compliance with CIP-003-2 R5. The entity self-certified non-compliance with CIP-003-2 R5 to Reliability*First*. The entity determined it did not document its program for managing access to protected Critical Cyber Asset (CCA) information pursuant to CIP-003-2 R5. Additionally, the entity did not maintain a list of designated personnel responsible for authorizing logical or physical access to protected information pursuant to CIP-003-2 R5.1. Reliability*First* determined that the entity failed to document a program for managing access to protected CCA information and failed to maintain a list of designated personnel responsible for authorizing logical or physical access to protected information.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the issue was a result of the entity's failure to document its program for managing access to CCAs information. It was a documentation failure because the entity had access controls in place during the duration of the issue which limited individuals' access to information regarding CCAs. The entity had physical and electronic access controls surrounding all information regarding CCAs that limited access to only authorized personnel. This included electronic access control lists as well as limiting physical access to badge access rooms only to individuals who had completed CIP training and a personnel risk assessment (PRA) in accordance with the entity's procedures. Also, the entity delegated authorizing responsibility to designated personnel; however, the entity failed to document a list of those responsible personnel.	The entity performed the following mitigating activities. The entity developed a list of designated personnel responsible for authorizing logical and physical access to protected CCAs information. The entity also made changes to its procedures in order to include procedures to manage access to protected CCA information. The entity communicated all updates to its procedures on managing protected CCA information with relevant personnel. The entity completed mitigation activities for the issue.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100912	CIP-004-2	R4	The entity is subject to compliance with CIP-004-2 R4. The entity self-certified non-compliance with Reliability Standard CIP-004-2 R4 to ReliabilityFirst. The entity discovered it had not maintained its access list of personnel with cyber or unauthorized physical access to Critical Cyber Assets (CCAs). The entity also discovered it had not included, in its access list, the specific electronic access rights for individuals with access rights to CCAs. Specifically, after two employees received CIP training and completed a personnel risk assessment (PRA) in accordance with the entity's procedure, the entity granted them access to CCAs but failed to include their names and access rights on its access list. Additionally, the entity included a compliance specialist on the access list even though the entity did not grant the compliance specialist access rights. Reliability*First* found that the entity failed to maintain its list of personnel with authorized cyber or authorized unescorted physical access to CCAs when it failed to timely to include two individuals with access rights and mistakenly included one individual on the list without access rights. Further, Reliability*First* determined that the entity failed to include, in its access list, the specific electronic access rights it granted to the two employees.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined this issue posed a minimal risk to the reliability of the bulk power system (BPS), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the issue was a result of a documentation error. It was a documentation error because, although the access lists were incomplete, actual physical and electronic access rights were accurate and up to date. All individuals with cyber or unescorted physical access to CCAs had received CIP training, and completed PRAs in accordance with the entity's procedure prior to the entity granting those individuals access rights. Additionally, there were no occurrences of access, physical or electronic, that were not properly authorized and documented by the entity.	The entity performed the following mitigating activities. The entity updated its access list to reflect all individuals with physical and electronic access rights and included detailed electronic access rights for each individual with electronic access rights. The entity also developed an improved documentation process to help ensure the access lists reflect the most up to date information concerning electronic and physical access rights to CCAs. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100914	CIP-006-2	R1	The entity is subject to compliance with CIP-006-2 R1. The entity self-certified non-compliance with CIP-006-2 R1 to Reliability*First*. The entity determined it did not document all sub-requirements of CIP-006-2 R1 in its physical security plan. Specifically, the entity did not document sub-requirement CIP-006 R1.1, that all Cyber Assets within an Electronic Security Perimeter did not reside within an identified Physical Security Perimeter, and where a completely enclosed ("six-wall") border cannot be established, the entity did not deploy and document alternative measures to control physical access to such Cyber Assets; R1.4, that an appropriate use of physical access controls as described in R4 including visitor pass management, response to loss and prohibition of inappropriate use of physical access controls were addressed; R1.5, that a review of access authorization requests and revocation of access authorization, in accordance with CIP-004-2 R4 were addressed; and R1.6, that continuous escorted access within the Physical Security Perimeter of personnel not authorized for unescorted access were addressed in its physical security plan. Reliability*First* determined that the entity failed to document sub-requirements of CIP-006-2 R1.1, R1.4, R1.5 and R1.6 in its physical security plan.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the issue was the result of a documentation error. It was a documentation error because, although the entity's physical security plan lacked proper documentation of the sub-requirements of CIP-006-2 R1, the entity implemented all the physical security controls required by CIP-006-2 R1.	The entity performed the following mitigating activities. The entity documented the sub-requirements of CIP-006-2 R1 at issue in its physical security plan. Additionally, the entity scheduled and performed training, highlighting the addition of the sub-requirements to its physical security plan, for all of its personnel. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201100921	CIP-003-2	R1	The entity is subject to compliance with CIP-003-2 R1. The entity self-certified non-compliance with Reliability Standard CIP-007-2 R5 to Reliability*First*; however, upon further review, Reliability*First* determined the appropriate Reliability Standard implicated in the issue was CIP-003-2 R1. The entity failed to implement its cyber security policy. Specifically, the entity's cyber security policy requires the entity to change its passwords every 90 days. The entity did not implement the 90-day password policy to address any particular risk, but rather the entity based the 90-day password policy on generally accepted good practice. According to its cyber security policy, the entity should have changed its passwords no later than 90 days from the date the entity had to comply with CIP-003-2 R1; however, the entity did not change its passwords until eight months later. Reliability*First* determined that the entity failed to implement its cyber security policy by not changing its passwords every 90 days.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the entity's cyber security policy is more stringent than that required by CIP-007-2 R5.3.3, which requires that a registered entity change its passwords at least annually. The entity did change its passwords annually, but failed to implement its internal cyber security policy, which mandated it change its passwords every 90 days.	The entity mitigated the issue by changing its passwords and updating its password management process to align with CIP-007 R5. The entity completed mitigation activities for the issue.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC201000593	VAR-002-1	R1	The entity submitted a Self-Report to Reliability*First*. The entity reported that one of its generators at its plant operated with an automatic voltage regulator in service, but automatically controlling VARs instead of voltage. The entity did not notify its Transmission Operator that it was not operating in automatic voltage control mode. Although operating staff had been informed of the requirement to operate in automatic voltage control mode through internal communications and operating procedures, an operator misunderstood the generator control panel and placed a voltage regulator at its plant into automatic VAR control mode instead of automatic voltage control mode. Another operator recognized the error and returned the unit to automatic voltage control mode later that same day. Reliability*First* determined that the entity had an issue with VAR-002-1 R1 by failing to notify its Transmission Operator when it operated outside automatic voltage control mode.	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), and did not pose a serious or substantial risk. The risk posed by the nature of this issue was mitigated by the following factors. Since the generator in question automatically controlled for VARs, voltage support to the BPS continued, although to a lesser degree. Additionally, the plant met all of the voltage schedules as provided by its Transmission Operator during the period of the issue. The generator in question also has a capacity of less than 100 MW and interconnects to the transmission system at a lower voltage. Finally, the entity represents that this generator is not called upon by its Transmission Operator to support transmission system voltage.	The entity mitigated this issue by modifying the screen display on the generator control panel of the voltage regulator unit to make the controls easier to use and to more clearly indicate the voltage regulation status. The entity also conducted refresher training for operators to review the requirements for automatic voltage regulation and operation of the generator control panel. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC201000433	VAR-002-1	R1	The entity submitted a Self-Report to Reliability*First.* The entity reported that it had been operating its Plant A units, with a combined generating capacity of less than 600 MW, out of automatic voltage control mode since the mandatory compliance deadline date. The entity also reported that operators at its Plant B, which has less than 600 MW of generating capacity, changed the automatic voltage regulator to reactive power mode without notification to the entity's Transmission Operator. The voltage regulator manufacturer for the voltage regulator used at the entity's Plant A issued a technical information letter that described how the labeling of a unit's voltage regulation status created the potential for operators to misread that status. Specifically, the label "Off" actually corresponded to a voltage control setting, but some operators misinterpreted the setting as disabling the automatic voltage regulator. This manufacturer recommended that users of its voltage regulators modify the labels displayed on the generator control panel to more clearly indicate the control status corresponding to the "Off" selection. Upon receiving this notification, the entity updated its operating procedures and generator control panel configuration for the affected units at Plant A and began a review of all its plants for compliance. As a result of the review, the entity discovered that based on guidance from another voltage regulator manufacturer, it had been operating its Plant B unit in both automatic voltage control mode and reactive power mode intermittently since it was subject to VAR-002-1. The entity revised procedures and trained personnel on proper operating practices, including a requirement to operate only in automatic voltage control mode; however, the entity found that it operated out of automatic voltage control mode at its Plant B. On this date, an operator referenced an out-of-date unit start-up procedure and erroneously placed the generator in reactive power mode. Within three hours, the entity placed the generator in automatic voltage control mode. The entity self-reported both the long-term incorrect operation and the operator error. Reliability*First* determined that the entity failed to notify its Transmission Operator when it operated outside automatic voltage control mode.	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), and did not pose a serious or substantial risk. The risk posed by the nature of this issue was mitigated by the following factors. Since the generators operated in reactive power mode, voltage support to the BPS continued, although to a lesser degree, while the generators were not in automatic voltage control mode. In addition, Plant B uses controls outside the automatic voltage regulator that adjust the automatic voltage regulator set point to maintain the specified interconnection voltage for longer-term changes in steady-state conditions. Both plants maintained their respective voltage schedule during the time period of the issue. Finally, during the time period of the issue, the Plant A units operated at 11.8% capacity factor.	The entity performed the following mitigating activities. For its Plant A, the entity modified the screen display on the generator control panel of the voltage regulator unit to make the controls easier to use and to more clearly indicate the voltage regulation status. The entity also revised plant operating procedures to remove uncertainty regarding automatic voltage regulator modes of operation, reviewed the revised unit start-up procedure with operators, and enhanced automatic voltage regulator alarms. For its Plant B, the entity made the same changes, and also modified several system alerts and messages to confirm the status of the automatic voltage regulator and alert the status to managers, operators and shift supervisors. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 8 (RFC_URE8)	NCRXXXXX	RFC201100988	PRC-005-1	R1	The entity is subject to compliance with PRC-005-1 R1. Reliability*First* conducted a compliance audit of the entity. At the compliance audit, Reliability*First* determined that the entity failed to provide the basis for maintenance and testing intervals for protective relays, voltage and current sensing devices, DC control circuitry, and associated communication systems in its Protection System maintenance and testing program (Program). The entity did include maintenance and testing intervals for these devices in its Program, but did not define the basis for those maintenance and testing intervals, as required by PRC-005-1 R1.1. The entity failed to document a basis for testing and maintenance for 15 of 16 Protection System devices but did document a basis for its single station battery bank.	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), and did not pose a serious or substantial risk. The risk posed to the reliability of the BPS by the foregoing facts and circumstances was mitigated by the following factors. Although the entity failed to document a basis for the maintenance and testing intervals in its Program, it did include maintenance and testing intervals in its Program. Moreover, the entity completed all maintenance and testing within the maintenance and testing intervals of its Program except for certain transmission relays, as noted in a separate enforcement action.	The entity performed the following mitigating activities. The entity added the basis for the maintenance and testing intervals for protective relays, voltage and current sensing devices, DC control circuitry, and associated communication systems to its Program. The entity mitigated this issue by incorporating the basis for all its testing intervals in its Program. The entity completed these mitigating activities.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC201000373	CIP-008-1	R1	The entity is subject to compliance with CIP-008-1 R1. Reliability*First* conducted a CIP Spot Check of the entity. Reliability*First* reviewed the entity's emergency incident and disturbance reporting procedure (Emergency Procedure Version 1) and determined it had not included roles and responsibilities of the incident response teams in the Emergency Procedure Version 1, pursuant to CIP-008-1 R1.2. The entity updated the Emergency Procedure Version 1 to define the roles and responsibilities of its response team (Emergency Procedure Version 2). Reliability*First* also reviewed the entity's Emergency Procedure Version 2 and determined it did not contain a provision for the entity to review the Emergency Procedure Version 2 at least annually, pursuant to CIP-008-1 R1.5. Rather than conducting, at minimum, an annual review of its Cyber Security Incident response plan, the entity stated it would "periodically" conduct a review of the Emergency Procedure Version 2. Reliability*First* determined that the entity had an issue with CIP-008-1 R1.2 by failing to include the roles and responsibilities of its response teams within Emergency Procedure Version 1. Additionally, Reliability*First* determined that the entity had an issue with CIP-008-1, R1.5 by failing to include a provision within Emergency Procedure 2 requiring, at minimum, an annual review.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that this was a documentation error. It was a documentation error because the entity had a procedure in place prior to the compliance enforcement date, that provided roles and responsibilities in the event of Cyber Security Incidents; however, the entity inadvertently referenced the incorrect procedure in its Emergency Procedure Version 1. The entity defined roles and responsibilities of response teams when it updated Emergency Procedure Version 1, almost a year before Reliability*First*'s Spot Check. Also while, the entity's Emergency Procedure Version 2 called for periodic, rather than annual, review of the plan, the entity represents that the periodic review of Emergency Procedure Version 2 would include an annual review.	The entity performed the following mitigating activities. The entity updated its Cyber Security Incident response plan to define the roles and responsibilities of its response team, and thereby corrected the issue with CIP-008-1 R1.2. The entity updated its Emergency Procedure Version 1 to include specific roles and responsibilities for its response team pursuant to CIP-008-1 R1.2. The entity also revised Emergency Procedure Version 2 to provide for, at minimum, an annual review. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC201100998	CIP-007-3	R4	The entity is subject to compliance with CIP-007-3 R4. The entity submitted a Self-Report to Reliability*First* identifying a possible issue with CIP-007-3 R4. The entity determined it had not used anti-virus software and other malware prevention software for 135 Critical Cyber Assets (CCAs), pursuant to CIP-007-3 R4, and did not request a Technical Feasibility Exception (TFE) for this issue. The entity believed the 135 CCAs were integrated components of the servers on which they reside, therefore did not require separate anti-virus software or other malware prevention tool; however, 133 of these CCAs were self-contained modules within the server that provide a separate network connection for IT personnel to remotely manage the server under emergency conditions. The remaining two CCAs run directly on server hardware without requiring an additional underlying operating system. These characteristics of the 135 CCAs necessitated that they have anti-virus software and other malware prevention tools. The 135 CCAs are subject to CIP-007-3 R4, for which the entity should have complied or, alternatively, submitted a TFE request to Reliability*First*. According to the entity, these 135 CCAs were incapable of using anti-virus software and other malware prevention tools; however, the entity did not request a TFE from Reliability*First* concerning this issue until seven months after the compliance enforcement date. Reliability*First* determined that the entity failed to use anti-virus software and other malware prevention tools to mitigate risk exposure to the 135 CCAs pursuant to CIP-007-3 R4.	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), and did not pose a serious or substantial risk. The risk to the reliability of the BPS was mitigated by the fact that the entity had compensating measures in place prior to the mandatory compliance date. These compensating measures were ultimately approved by Reliability*First*. Specifically, the entity installed firewalls at the perimeter of the Electronic Security Perimeter (ESP) with an intrusion prevention system that can detect and prevent many types of malware from propagating. The entity also installed virus protection on workstations and servers as well as firewall software on its workstations. The entity stores the passwords for the CCAs securely in a server password database that is restricted to authorized personnel. Finally, the entity limits administrative access to the CCAs to a small group of support personnel to further minimize risk exposure. These compensating measures were in place for the entire time period of the issue.	The entity mitigated this issue by submitting its TFE requests for the CCAs at issue. Reliability*First* subsequently accepted and approved the entity's TFE requests. The entity completed mitigation activities for the issue.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC20100529	FAC-008-1	R1	SERC_URE1 self-reported that it did not have a documented Facility Ratings Methodology (FRM) from its date of registration, until approximately one month later. SERC_URE1 documented its FRM; however, the procedure did not include: 1. The statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility; 2. Normal and Emergency Ratings for all the applicable equipment; and 3. Relay protective devices and series and shunt compensation devices.	SERC staff 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 because: 1. SERC_URE1 identified the generator as the most limiting element prior to documenting its FRM; 2. Normal and Emergency ratings were included for some of the equipment; and 3. SERC_URE1 does not own series or shunt compensation devices.	SERC staff verified that SERC_URE1 revised its FRM to: 1. Include a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility; 2. Include normal and emergency ratings for all the applicable equipment; and 3. Include consideration statements for all the devices listed in the Standard, even if not owned by the entity.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC201000597	PRC-005-1	R2	SERC_URE2 self-reported that nine batteries at its generation facilities were not being tested in accordance with the defined intervals of its Protection System maintenance and testing program. While performing its Protection System devices inventory, SERC_URE2 identified seven Protective Relays that did not have previous maintenance and testing records. In total, 1.1% total Protection System devices were not tested within the defined interval or had no previous maintenance and testing records.	SERC staff 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 because the station batteries and the relays are constantly monitored as part of SERC_URE2's system which would have indicated potential problems with these devices.	SERC staff verified that SERC_URE2 tested the batteries and relays that were out of compliance.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC201000632	VAR-002-1.1a	R1	SERC_URE3 self-reported that it failed to operate each generator in the automatic voltage control mode, as required. Specifically, one of SERC_URE3's units was inadvertently changed by the operator from automatic voltage control mode to manual mode without previously notifying its Transmission Operator (TOP). SERC_URE's unit operated in manual mode for four hours prior to shut down. SERC_URE3 reported the change in status to the TOP approximately a week later.	SERC staff 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 because: 1. The unit maintained its voltage schedule; 2. The incident involved only one unit at the facility, which consists of three units with a total capacity of over 500 MW; and 3. After reviewing its records, SERC_URE3 did not identify any other instance of its generators operating with its AVR out of service without appropriate communication to its TOP.	SERC staff verified that SERC_URE3: 1. Moved the AVR switch to a different computer screen in order to prevent an inadvertent change from AVR to Manual mode; 2. Added a computer screen indicator flag to remind operators to notify the TOP of a change in status; and 3. Trained SERC_URE3 plant operations staff regarding the appropriate actions to take in the event of status change.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC201000633	VAR-002-1.1a	R3	SERC_URE3 self-reported that it did not notify its Transmission Operator (TOP) of the status change in the automatic voltage regulator (AVR) operation, as required. Specifically, one of SERC_URE3's units was inadvertently changed by the operator from automatic voltage control mode to manual mode and SERC_URE3 did not notify its associated TOP within 30 minutes. SERC_URE3's unit operated in manual mode for four hours prior to shut down. SERC_URE3 reported the change in status to the TOP approximately a week later.	SERC staff 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 because: 1. The unit maintained its voltage schedule; 2. The incident involved only one unit at the facility, which consists of three units with a total capacity of over 500 MW; and 3. After reviewing its records, SERC_URE3 did not identify any other instance of its generators operating with its AVR out of service without appropriate communication to its TOP.	SERC staff verified that SERC_URE3: 1. Moved the AVR switch to a different computer screen in order to prevent an inadvertent change from AVR to Manual mode; 2. Added a computer screen indicator flag to remind operators to notify the TOP of a change in status; and 3. Trained SERC_URE3 plant operations staff regarding the appropriate actions to take in the event of status change.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1) City of Bentonville, Arkansas (Bentonville)	NCRXXXXX	SPP201100450	CIP-001-1	R1	SPP_URE1 self-reported an issue with CIP-001-1 R1-R4. SPP_URE1 reported that it did not have a documented procedure for the recognition of sabotage and for making its operating personnel aware of sabotage events and multi-site sabotage affecting larger portions of the Interconnection, as required by R1.	SPP RE has determined that SPP_URE1's issue with CIP-001-1 R1 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SPP_URE1 does not own or operate transmission facilities over 100 kV. It is a small municipal electric utility with fewer than 18,000 electric customers, and its system peak load was during the summer of 2011. Furthermore, SPP_URE1 stated that its operating personnel regularly patrolled its facilities, and were instructed to report any suspicious activities, *e.g.* , sabotage, to the local police and rely on them to handle the situation. Based on SPP_URE1's small customer base and load and its lack of transmission facilities it is improbable that SPP_URE1 would be a target of sabotage or that any sabotage on the SPP_URE1 system would result in a serious or substantial impact on the BPS. The informal policies SPP_URE1 had in place covering sabotage also mitigated any potential impact. Accordingly, SPP RE determined this issue with CIP-001-1 R1 posed a minimal risk to the BPS.	SPP_URE1 developed and implemented a comprehensive sabotage reporting procedure used for the recognition of and for making operating personnel aware of sabotage events on SPP_URE1 facilities and multi-site sabotage events that may affect larger portions of the Interconnections. The procedure contains the communications, reporting and response guidelines to enable SPP_URE1's operating personnel to appropriately respond to sabotage events, and addresses the requirements of CIP-001-1 R1-R4. SPP_URE1 certified mitigation as being complete, and SPP RE verified mitigation as complete.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1) City of Bentonville, Arkansas (Bentonville)	NCRXXXXX	SPP201100451	CIP-001-1	R2	SPP_URE1 self-reported an issue with CIP-001-1 R1-R4. Because SPP_URE1 did not have a documented sabotage reporting procedure as required by CIP-001-1 R1, it did not have documented procedure for communicating information concerning sabotage to other parties in the Interconnection, as required by R2.	SPP RE has determined that SPP_URE1's issue with CIP-001-1 R2 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SPP_URE1 does not own or operate transmission facilities over 100 kV. It is a small municipal electric utility with fewer than 18,000 electric customers, and its system peak load was during the summer of 2011. Furthermore, SPP_URE1 stated that its operating personnel regularly patrolled its facilities, and were instructed to report any suspicious activities, *e.g.* , sabotage, to the local police and rely on them to handle the situation. Based on SPP_URE1's small customer base and load and its lack of transmission facilities it is improbable that SPP_URE1 would be a target of sabotage or that any sabotage on the SPP_URE1 system would result in a serious or substantial impact on the BPS. The informal policies SPP_URE1 had in place covering sabotage also mitigated any potential impact. Accordingly, SPP RE determined this issue posed a minimal risk to the BPS.	SPP_URE1 developed and implemented a comprehensive sabotage reporting procedure used for the recognition of and for making operating personnel aware of sabotage events on SPP_URE1 facilities and multi-site sabotage events that may affect larger portions of the Interconnections. The procedure contains the communications, reporting and response guidelines to enable SPP_URE1's operating personnel to appropriately respond to sabotage events, and addresses the requirements of CIP-001-1 R1-R4. SPP_URE1 certified mitigation as being complete, and SPP RE verified mitigation as complete.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1) City of Bentonville, Arkansas (Bentonville)	NCRXXXXX	SPP201100452	CIP-001-1	R3	SPP_URE1 self-reported an issue with CIP-001-1 R1-R4. Because SPP_URE1 did not have a documented sabotage reporting procedure as required by CIP-001-1 R1, it did not have sabotage response guidelines for its operating personnel, as required by R3.	SPP RE has determined that SPP_URE1's issue with CIP-001-1 R3 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SPP_URE1 does not own or operate transmission facilities over 100 kV. It is a small municipal electric utility with fewer than 18,000 electric customers, and its system peak load was during the summer of 2011. Furthermore, SPP_URE1 stated that its operating personnel regularly patrolled its facilities, and were instructed to report any suspicious activities, *e.g.* , sabotage, to the local police and rely on them to handle the situation. Based on SPP_URE1's small customer base and load and its lack of transmission facilities it is improbable that SPP_URE1 would be a target of sabotage or that any sabotage on the SPP_URE1 system would result in a serious or substantial impact on the BPS. The informal policies SPP_URE1 had in place covering sabotage also mitigated any potential impact. Accordingly, SPP RE determined this issue posed a minimal risk to the BPS.	SPP_URE1 developed and implemented a comprehensive sabotage reporting procedure used for the recognition of and for making operating personnel aware of sabotage events on SPP_URE1 facilities and multi-site sabotage events that may affect larger portions of the Interconnections. The procedure contains the communications, reporting and response guidelines to enable SPP_URE1's operating personnel to appropriately respond to sabotage events, and addressed the requirements of CIP-001-1 R1-R4. SPP_URE1 certified mitigation as being complete, and SPP RE verified mitigation as complete.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1) City of Bentonville, Arkansas (Bentonville)	NCRXXXXX	SPP201100453	CIP-001-1	R4	SPP_URE1 self-reported an issue with CIP-001-1 R1-R4. Because SPP_URE1 did not have a documented sabotage reporting procedure as required by CIP-001-1 R1, it did not have procedures for communicating with or communications contacts for the local FBI office, as required by R4.	SPP RE has determined that SPP_URE1's issue with CIP-001-1 R4 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). SPP_URE1 is registered as a Load Serving Entity and Distribution Provider only, and does not own or operate transmission facilities over 100 kV. It is a small municipal electric utility with fewer than 18,000 electric customers, and its system peak load was 153 MW during the summer of 2011. Furthermore, SPP_URE1 stated that its operating personnel regularly patrolled its facilities, and were instructed to report any suspicious activities, *e.g.* , sabotage, to the local police and rely on them to handle the situation. Based on SPP_URE1's small customer base and load and its lack of transmission facilities it is improbable that SPP_URE1 would be a target of sabotage or that any sabotage on the SPP_URE1 system would result in a serious or substantial impact on the BPS. The informal policies SPP_URE1 had in place covering sabotage also mitigated any potential impact. Accordingly, SPP RE determined this issue posed a minimal risk to the BPS.	SPP_URE1 developed and implemented a comprehensive sabotage reporting procedure used for the recognition of and for making operating personnel aware of sabotage events on SPP_URE1 facilities and multi-site sabotage events that may affect larger portions of the Interconnections. The procedure contains the communications, reporting and response guidelines to enable SPP_URE1's operating personnel to appropriately respond to sabotage events, and addresses the requirements of CIP-001-1 R1-R4. SPP_URE1's mitigation plan was assigned Mitigation Plan No. MIT-10-3575. SPP_URE1 certified mitigation as being complete, and SPP RE verified mitigation as complete.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201100531	EOP-008-0	R1.7	SPP_URE2 self-reported a potential issue with EOP-008-0 R1/R1.7. SPP_URE2 could not provide evidence that it had updated or reviewed its transmission systems Emergency Operation Plans, its plan to continue reliability operations in the event its control center became inoperable, which must be updated and reviewed annually, in 2010. Prior to its Self-Report, SPP_URE2 had reviewed and updated its transmission system Emergency Operations Plan in the fall of 2009.	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). SPP_URE2 had a document that acted as its plan for a loss of control center functionality as required by EOP-008-0 R1. Although SPP_URE2 could not provide evidence that it had reviewed or updated this document for the year 2010, SPP_URE2 indicated that there were no substantial changes made other than updating personnel information. Because SPP_URE2 did have a plan in place, and because that plan had not substantively changed so as to change the overall functional process, SPP RE determined this lack of review to be a minimal risk to the BPS.	The specific tasks initiated to accomplish the plan are as follows: Review and update the transmission system Emergency Operation Plans. The actions initiated to prevent recurrence are as follows: (1) A mechanism was implemented to remind personnel responsible for updating this document to ensure review and approval cycle is completed. (2) Developed and implemented a transmission system operations documentation review procedure that at a minimum includes an inventory of transmission system operations documents that need periodic updating as required in the NERC Reliability Standards as well as an update schedule, review and approval deadline for each document.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201100533	MOD-019-0	R1	SPP_URE2 self-reported a potential issue with MOD-019-0 R1 regarding the annual reporting of forecasts of interruptible demands and Direct Control Load Management (DCLM) data to SPP and NERC as specified by the documentation in MOD-016-1.1 R1. SPP_URE2 stated that it had unintentionally provided an inaccurate forecast of SPP_URE2's 2010 interruptible demands and DCLM data to the Southwest Power Pool Regional Reliability Organization (SPP RRO) and NERC.	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 data that SPP_URE2 provided was used for SPP RRO long term forecasting as opposed to real-time operations (the data for real-time operations was obtained through different channels and is not implicated by this issue). Furthermore, SPP_URE2 stated that the year 2010 was the only year that it did not provide its annual forecasts of interruptible demands and direct control load management. SPP_URE2 states that it submitted the data accurately in the years previous to 2010 and again in March 2011. The long term forecasts were through the year 2019, and the submittal of the correct data in March 2011 corrected any discrepancies that might have resulted in the 2010 error.	The specific tasks performed to accomplish the plan were as follows: Confirm with SPP planning personnel to ensure understanding of report submissions for interruptible demand and DCLM data. Require management review of EIA-411 reports prior to submittal to SPP. The actions taken to prevent recurrence were as follows: Develop specific written procedures for completing Form EIA-411.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP_URE3)	NCRXXXXX	SPP201100532	EOP-008-0	R1.7	SPP_URE3 self-reported a potential issue with EOP-008-0 R1/R1.7. SPP_URE3 could not provide evidence that it had updated or reviewed its transmission systems Emergency Operation Plans, its plan to continue reliability operations in the event its control center became inoperable, which must be updated and reviewed annually, in 2010. Prior to its Self Report, SPP_URE3 had reviewed and updated its transmission systems Emergency Operations Plan in the fall of 2009.	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). SPP_URE3 had a document that acted as its plan for a loss of control center functionality as required by EOP-008-0 R1. Although SPP_URE3 could not provide evidence that it had reviewed or updated this document for the year 2010, SPP_URE3 indicated that there were no substantial changes made other than updating personnel information. Because SPP_URE3 did have a plan in place, and because that plan had not substantively changed so as to change the overall functional process, SPP RE determined this lack of review to be a minimal risk to the BPS.	The specific tasks initiated to accomplish the plan are as follows: Review and update the transmission system Emergency Operation Plans The actions initiated to prevent recurrence are as follows: (1) A mechanism was implemented to remind personnel responsible for updating this document to ensure review and approval cycle is completed. (2) Developed and implemented a transmission system operations documentation review procedure that at a minimum includes an inventory of transmission system operations documents that need periodic updating as required in the NERC Reliability Standards as well as an update schedule, review and approval deadline for each document.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP_URE3)	NCRXXXXX	SPP201100534	MOD-019-0	R1	SPP_URE3 self-reported a potential issue with MOD-019-0 R1 regarding the annual reporting of forecasts of interruptible demands and Direct Control Load Management (DCLM) data to SPP and NERC as specified by the documentation in MOD-016-1.1 R1. SPP_URE3 stated that it had unintentionally provided an inaccurate forecast of SPP_URE3's 2010 interruptible demands and DCLM data to the Southwest Power Pool Regional Reliability Organization (SPP RRO) and NERC.	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 data that SPP_URE3 provided was used for SPP RRO long term forecasting as opposed to real-time operations (the data for real-time operations was obtained through different channels and is not implicated by this issue). Furthermore, SPP_URE3 stated that the year 2010 was the only year that it did not provide its annual forecasts of interruptible demands and direct control load management. SPP_URE3 states that it submitted the data accurately in the years previous to 2010 and again in March 2011. The long term forecasts were through the year 2019, and the submittal of the correct data in March 2011 corrected any discrepancies that might have resulted in the 2010 error.	The specific tasks performed to accomplish the plan were as follows: Confirm with SPP planning personnel to ensure understanding of report submissions for interruptible demand and DCLM data. Require management review of EIA-411 reports prior to submittal to SPP. The actions taken to prevent recurrence were as follows: Develop specific written procedures for completing Form EIA-411.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity (TRE_URE1)	NCRXXXXX	TRE201000119	FAC-009-1	R1	During an audit, Texas RE determined that TRE_URE1 failed to produce any evidence of a documented Facility Ratings Methodology prior to April 30, 2009, nor did TRE_URE1 provide documentation of any calculations of Facility Ratings (based on any documented or undocumented Facility Ratings Methodology) that were performed prior to April 30, 2009.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because TRE_URE1 had already developed and had been submitting its Facility Ratings to ERCOT ISO. Even after TRE_URE1 developed an official Facility Ratings Methodology, the ratings being reported to ERCOT ISO remained identical to the year before, demonstrating that the lack of documentation had minimal impact/risk to its operation.	The Mitigation Plan was completed and verified by Texas RE. TRE_URE1 employed a third party entity to develop its entire Compliance Program including the development and documentation of Facility Rating Methodology and Facility Rating calculation based off of this Methodology. TRE_URE1 provided the Facility Ratings to Texas RE during the Audit. Texas RE has verified that these ratings were developed according to the Facility Ratings Methodology provided for FAC-008-1. These ratings were also in place as of April 30, 2009.

Attachment A-1

November 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201103046	CIP-003-2	R5	WECC_URE1 self-reported that it had failed to implement its access control program pursuant to CIP-003-2 R5. As part of WECC_URE1's access controls related to accessing Critical Cyber Asset (CCA) information, WECC_URE1 maintains a list of individuals that WECC_URE1 authorized to access such information. In this case, a WECC_URE1 engineer had a business need to view CCA information. An individual that WECC_URE1 designated to grant access to such information invited the engineer into a meeting where CCA information was displayed (projected) on a wall. Although the power production engineer had a business need to view this information, had the appropriate training to properly utilize this information, and was intentionally granted access by a an individual responsible for granting access to this information, WECC_URE1 did not implement its documented program for managing access to protected CCA information. Specifically, WECC_URE1's documented program establishes that WECC_URE1 will place individuals on a list prior to being granted such access. In this case, WECC_URE1 place the engineer on the list after the meeting. The person who manages access (as required in CIP-003 R5.1) to the protected information in scope invited the power production engineer to attend the meetings before the engineer was placed on WECC_URE1's list as an individual authorized to view protected information.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because even though allowing access to an information related to an entity's CCAs could allow such information to be unintentionally misused or used with malicious intent, in this case WECC_URE1 provided significant protections to such information. There is no evidence to suggest WECC_URE1 allowed access to such information without taking appropriate precautions to protect the information and guard against possible misuse of the information. An individual responsible for granting access to the information invited a long-time employee with a business need to view the information to a meeting where the individual could view the information. This individual had a personnel risk assessment, CIP training, and had a legitimate business need to access the information, but was not on WECC_URE1's authorized list to view such information. WECC_URE1 added the individual to the authorized list following the meeting. Additionally, the individual in scope was only able to view information related to Critical Assets while at the meeting and only viewed the information projected on a wall. The individual did not have electronic or physical access to the information, could not remove the information from the room, and remains an employee in good standing.	WECC_URE1 placed the engineer on the list of individuals authorized to view protected information.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201103049	VAR-002-WECC-1	R1	WECC_URE2 submitted a Periodic Data Submittal stating that it had failed to maintain automatic voltage regulators (AVRs) in service and in automatic voltage control mode 98% of all operating hours in a calendar quarter for generators synchronous within the Western Interconnection. At 21:26, WECC_URE2 took the AVR offline on the steam turbine at one of WECC_URE2's generating station. The steam turbine operated with the AVR out of service for approximately 105 hours, resulting in WECC_URE2 operating the AVR less than 98 percent (i.e., approximately 95 percent of the generator's on-time for third quarter 2011). WECC_URE2 discovered and corrected the AVR status five days later. The AVR outage reduced the AVR operation to under 98% of generator on-line time for the 3rd quarter.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because while the result of operating without AVR in automatic voltage control mode could be that the generator would not respond to changes in voltage by increasing or decreasing VAR output, which could result in insufficient reactive reserves during disturbances; in this case WECC_URE2 operated its remaining generators with the AVR in service, in voltage control mode, set to respond effectively to voltage deviations. Therefore the issue with the steam turbine represented a fraction of WECC_URE2's total generation and an even smaller fraction of the total generating capacity available to WECC_URE2's function. Further, the entirety of the generating station is only at approximately 500 MW and the steam turbine is rated at less than 200 MW.	WECC_URE2 placed the AVR in service and in automatic voltage control mode after five days.

Document Content(s)