Federal Energy Regulatory Commission
Washington, D.C. 20426

January 31, 2022

FOIA No. FY19-30 (RC13-9)
Fifty Sixth Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated January 20, 2022, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC13-9, along with the names of nine (9) 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 RC13-9

With respect to the remaining identities of UREs contained in RC13-9, before making a determination as to whether this information is appropriate for release under

[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.

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC13-9 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 12:13:09 -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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC13-9

Clewiston, City of (CLE)-.pdf page 25
Noble Altona Windpark, LLC-.pdf page 26
Noble Bliss Windpark, LLC-.pdf page 26
Noble Chateaugay Windpark, LLC-.pdf page 26-27
Noble Clinton Windpark, LLC-.pdf page 27
Noble Ellenburg Windpark, LLC-.pdf page 27
Noble Wethersfield Windpark, LLC-.pdf page 27
CMS Generation Michigan Power, L.L.C. (CMSMP)-.pdf page 28
CPS Energy - DP-LSE-TO-TOP-TP (CPS)-.pdf page 31

May 30, 2013

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. RC13-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find, Fix, Track and Report[1] (FFT Spreadsheet) in Attachment A regarding 53 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 93 possible violations[5] of 20 Reliability Standards that posed a minimal risk 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 certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 93 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

[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.

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is an 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 certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, a spot check, a random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

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

[6] *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) ("March 15, 2012 CEI Order"); *see also 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).
[8] *See* 18 C.F.R § 39.7(d)(4).

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.

Notice of Completion of Enforcement Action

In accordance with section 5.10 of the CMEP, and the Commission's March 15, 2012 CEI Order, provided that the Commission has not issued a notice of review of a specific matter included in this filing, notice is hereby provided that, sixty-one days after the date of this filing, enforcement action is complete with respect to all remediated issues included herein and any related data holds are released only as to that particular remediated issue.

Pursuant to the Commission order referenced above, both the Commission and NERC retain the discretion to review a remediated issue after the above referenced sixty-day period if it finds that FFT treatment was obtained based on a material misrepresentation of the facts underlying the FFT matter. Moreover, to the extent that it is subsequently determined that the mitigation activities described herein were not completed, the failure to remediate the issue will be treated as a continuing possible violation of a Reliability Standard requirement that is not eligible for FFT treatment.

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.

[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).

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.

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) FFT 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 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Sonia C. Mendonca* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 edwin.kichline@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/ Sonia C. Mendonca

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

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

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

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

cc: Entities listed in Attachment B

NERC

Attachment a

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

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR MAY 2013
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

Stacy Dochoda*
President and Chief Executive Officer
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 600
Tampa, Florida 33607-8411
(813) 207-7960
(813) 289-5646 – facsimile
sdochoda@frcc.com

Linda Campbell*
VP and Executive Director Standards & Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 600
Tampa, Florida 33607-8411
(813) 207-7961
(813) 289-5646 – facsimile
lcampbell@frcc.com

Barry Pagel*
Director of Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 600
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5646 – facsimile
bpagel@frcc.com

For MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Vice President of Regulatory Affairs and Enforcement
Midwest Reliability Organization
380 St. Peter Street, Suite 800
Saint Paul, MN 55102
(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, NY 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 Analytics & Enforcement
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
bob.wargo@rfirst.org

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

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

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

FOR SERC:

John R. Twitchell*
VP and Chief Program Officer
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8205
(704) 357-7914 – facsimile
jtwitchell@serc1.org

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

Maggie A. Sallah*
Senior Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7778
(704) 357-7914 – facsimile
msallah@serc1.org

James M. McGrane*
Legal Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7787
(704) 357-7914 – facsimile
jmcgrane@serc1.org

Andrea B. Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

FOR SPP RE:

Ron Ciesiel*
General Manager
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 614-3265
(501) 482-2025 – facsimile
rciesiel.re@spp.org

Joe Gertsch*
Manager of Enforcement
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 688-1672
(501) 482-2025 – facsimile
jgertsch.re@spp.org

Peggy Lewandoski*
Paralegal & SPP RE File Clerk
Southwest Power Pool Regional Entity
201 Worthen Drive
Little Rock, AR 72223
(501) 482-2057
(501) 482-2025 – facsimile
spprefileclerk@spp.org

FOR TEXAS RE:

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

Derrick Davis*
Senior Corporate Counsel
Texas Reliability Entity, Inc.
805 Las Cimas Parkway
Suite 200
Austin, TX 78746
(512) 583-4923
(512) 233-2233 – facsimile
derrick.davis@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

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

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7674
(801) 883-6894 – facsimile
rarredando@wecc.biz

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RC13-___-000

NOTICE OF FILING
May 30, 2013

Take notice that on May 30, 2013, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding fifty-three (53) 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

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)	Covanta Southeastern Florida Renewable Energy (SEFLOR), LTD. (COVS)	NCR11009	FRCC2013011686	VAR-002-1.1b	R1	On January 9, 2013, COVS submitted a Self-Report to FRCC stating that, as a Generator Operator, it had an issue with VAR-002-1.1b R1. On January 1, 2013, COVS notified Progress Energy, the Balancing Authority, and Florida Power & Light Company, the Transmission Operator, that Turbine Generator #2 (T/G #2), had been brought back online; however plant personnel failed to inform its respective BA and TOP that the Turbine Generator #2 automatic voltage regulator (AVR) was in manual operation instead of the required automatic mode from 9:57 p.m. on January 1, 2013 to 3:27 a.m. on January 2, 2013.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. COVS notified the BA and TOP that T/G #2 had been brought back online and the BA and TOP would have been able to monitor the line voltage of the units through the supervisory control and data acquisition system. In addition the COVS facility maintained the required voltage schedule and the facility's total generation is only 60 MW. Furthermore, the AVR was in manual for a short time, approximately four hours.	To mitigate this issue, COVS: 1) notified the BA and TOP at 9:30 a.m. on January 2, 2013 that the AVR had been in manual from 9:57 p.m. on January 1, 2013 to 3:27 a.m. on January 2, 2013; 2) terminated conductors properly in the 501 Circuit Breaker. 3) conducted NERC compliance refresher training for all responsible personnel; 4) posted a summary of NERC reporting requirements in both the turbine control room and the main control room, along with updated subject matter expert (SME) contact information. 5) ensured that all SMEs are aware of the need to be available for plant support; 6) implemented written disciplinary action for the shift supervisor responsible for communicating AVR manual status; 7) Alstom, a third-party vendor, SME to verify logic of AVR sequences on Turbine Generator #1 and Turbine Generator #2. 8) revised its Turbine Generator Standard Operating Procedures (SOP) that incorporate NERC-specific actions. 9) incorporated a visual message to accompany distributed control system alarming when AVR falls out of automatic operation mode; and 10) retrained all affected personnel on the revised SOP March 31, 2013.
Florida Reliability Coordinating Council, Inc. (FRCC)	Covanta Southeastern Florida Renewable Energy (SEFLOR), LTD. (COVS)	NCR11009	FRCC2013011690	VAR-002-1.1b	R3	On January 9, 2013, COVS submitted a Self-Reported to FRCC stating that, as a Generator Operator, it had an issue with VAR-002-1.1b R3. On January 1, 2013, COVS notified Progress Energy, the Balancing Authority (BA), and Florida Power & Light Company, the Transmission Operator (TOP), that Turbine Generator #2, had been brought back online; however, plant personnel failed to inform its respective TOP that the Turbine Generator #2 automatic voltage regulator (AVR) was in manual operation instead of the required automatic mode from 9:57 p.m. on January 1, 2013 to 3:27 a.m. on January 2, 2013. Therefore, COVS failed to notify its TOP that of change in AVR status within 30 minutes of the change as required by the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. COVS notified the BA and TOP that T/G #2 had been brought back online and the BA and TOP would have been able to monitor the line voltage of the units through the supervisory control and data acquisition system. In addition the COVS facility maintained the required voltage schedule and the facility's total generation is only 60 MW. Furthermore, the AVR was in manual for a short time, approximately four hours.	To mitigate this issue, COVS: 1) notified the BA and TOP at 9:30 a.m. on January 2, 2013 that the AVR had been in manual from 9:57 p.m. on January 1, 2013 to 3:27 a.m. on January 2, 2013; 2) terminated conductors properly in the 501 Circuit Breaker. 3) conducted NERC compliance refresher training for all responsible personnel; 4) posted a summary of NERC reporting requirements in both the turbine control room and the main control room, along with updated subject matter expert (SME) contact information. 5) ensured that all SMEs are aware of the need to be available for plant support; 6) implemented written disciplinary action for the shift supervisor responsible for communicating AVR manual status; 7) Alstom, a third-party vendor, SME to verify logic of AVR sequences on Turbine Generator #1 and Turbine Generator #2. 8) revised its Turbine Generator Standard Operating Procedures (SOP) that incorporate NERC-specific actions. 9) incorporated a visual message to accompany distributed control system alarming when AVR falls out of automatic operation mode; and 10) retrained all affected personnel on the revised SOP March 31, 2013.
Florida Reliability Coordinating Council, Inc. (FRCC)	Vero Beach, City of (VERO)	NCR00079	FRCC2012010474	PER-002-1	R2; R2.1	During a Compliance Audit, conducted on June 8, 2012, FRCC auditors found that VERO was unable to provide sufficient evidence to demonstrate that VERO has a training program for all operating personnel in positions that have the primary responsibility, either directly or through communications with others, for the real-time operation of the interconnected Bulk Electric System (BES), as required by PER-002-1 R2.1. Specifically, the supervisor of the transmission and distribution system operations job description lists the principal responsibilities of that person as: plans, organizes, controls and provides direction of electrical system dispatch operations including supervisory control and data acquisition operations. This person should have been, but was not listed in the training program as someone requiring training. Due to the job description as someone with primary responsibilities for the real-time operation of the interconnected BES, the person should have been included in the training program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The affected individual did receive training and was just not documented as someone who required training. In addition, VERO is a small municipal with 14 miles of 138 kV transmission (less than 1% of regional transmission) serving 210 MW peak load and no registered generation (144 MW of non-registered generation connected at 69 kV).	To mitigate this issue, VERO: 1) edited the job description of the supervisor of the transmission and distribution system operations to accurately reflect the duties of that position, in that this position does not have the primary responsibility, either directly or through communication with others, for the real-time operation of the interconnected BES, and to not require that position to have training.
Florida Reliability Coordinating Council, Inc. (FRCC)	Vero Beach, City of (VERO)	NCR00079	FRCC2012010476	PER-002-1	R4	During a Compliance Audit on June 8, 2012, FRCC auditors found that VERO was unable to provide sufficient evidence to demonstrate that for personnel identified in PER-002-1 R4, VERO provided its operating personnel at least five days per year of training and drills using realistic simulations of system emergencies, in addition to other training required to maintain qualified operating personnel. Specifically, two out of six system operators completed 26.5 hours of the required 32 hours using realistic simulations of system emergencies in 2010. The issue occurred due to a miscalculation by VERO of the hours each person completed.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. VERO is contained within a much larger Balancing Authority/Transmission Operator (Florida Power & Light Company) footprint. The affected employees were long-term employees. One employee began working for VERO in 1996 and the other began in 2006. Although VERO's operations staff was not adequately trained and as a result, might make operational errors, such errors would more likely only impact VERO's own load and non-registered generation. Also, while the hours were not met in 2010, they were met in 2009 and 2011 and missed by only 5.5 hours each person in 2010.	To mitigate this issue, VERO: 1) revised its PER-002 R4 EOP training documentation improvements; 2) took steps to ensure that its operators receive the required 32 hours of EOP training since 2010. All operators received the required training in 2011 and all are on schedule to receive the required training in 2012; 3) implemented documentation to identify and schedule the 32 hours of EOP training required annually and to record the EOP training delivered for each operator; and 4) performed a review by the supervisor of system operations, on an ongoing basis, of the documentation at least quarterly to assure that all operators will receive the required training.

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)	Lincoln Electric System (LES)	NCR01001	MRO2012011486	BAL-005-0.1b	R16	On September 27, 2012, LES, as a Balancing Authority, self-reported noncompliance with BAL-005-0.1b R16. Specifically, LES failed to sample data at the same periodicity with which Area Control Error (ACE) is calculated and also failed to flag missing or bad data for operator display and archival purposes. LES performed an internal review of all 15 inputs (14 Tie Line inputs and a frequency source input) into its ACE equation in order to ensure that all 15 inputs were being scanned at an interval equal to or greater than its ACE calculation rate, every two seconds. During the review, LES discovered that 1 of its 15 ACE inputs was scanning at a rate of once every four seconds instead of once every two seconds. This setting discrepancy caused one of the Tie Lines to provide two second old "stale" data into the ACE calculation every other scan. Therefore, half of the ACE calculations received all of the coincident data from all 15 inputs and the other half of the ACE calculations received coincident data from 14 of the 15 inputs. LES became aware of this scan rate discrepancy on September 19, 2012, and after investigating, LES staff changed the scan rate back to every two seconds on the same day, September 19, 2012. Over the next two days, an in-depth investigation was performed in order to determine why the scan rate change was made and when it was made. LES discovered that the scan rate change was made on March 18, 2011 in order to troubleshoot one of its Tie Line remote terminal units (RTUs). Although the scan rate frequency was determined not to be the cause of the RTU issue, the substation technician decided to leave the scan rate at every four seconds in order to reduce the traffic on the RTU.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). One of the 15 inputs was scanned at a rate of every four seconds rather than every two seconds, and LES mitigated the issue by reconfiguring the setting within two hours of discovering the scan rate discrepancy. Additionally, LES collects the data necessary in the calculation of ACE every two seconds, which is below the six second requirement referenced in BAL-005-0.1b R8. Therefore, MRO determined that this issue posed a minimal risk to the BPS due to the extremely small error that this scan rate discrepancy introduced into LES's ACE calculation.	To mitigate this issue, LES: 1) performed a full internal investigation to determine the scope of the issue; and 2) implemented notes and pushpins on the RTU configuration page, in addition to all applicable Tie Lines and frequency source inputs, alerting users that the sampling rate should remain at two seconds in compliance with BAL-005-0.1b R16.
Northeast Power Coordinating Council, Inc. (NPCC)	ANP Bellingham Energy Company (ANP Bellingham)	NCR07006	NPCC2011008239	PRC-005-1	R2	On September 22, 2011, ANP Bellingham submitted a Self-Report to NPCC stating that, as a Generator Owner, it had an issue with PRC-005-1 R2. ANP Bellingham conducted an internal assessment of its relay testing and determined that, for 2 out of 17 of its instrument transformers, there were missing test certificates from 2007, the previous defined testing four year interval. In addition, during the previous testing interval, the contractor who performed the testing did not provide any test certificates for relay functional checks. Although the planned maintenance form clearly stated that each relay was to be calibrated, a functional trip test was to be performed, and the maintenance activity was completed, the formal documentation was missing.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. While it appears that the testing interval has been exceeded, this was a documentation issue and the affected relays were actually tested and maintained within the defined interval.	To mitigate this issue, ANP Bellingham: 1) performed all the testing to correct the deficiencies noted above; and 2) revised its Protection System testing procedure to require the contractor deliver a complete and accurate report before final payment is made
Northeast Power Coordinating Council, Inc. (NPCC)	NAES Corporation - Lockport (NAES Lockport)	NCR07167	NPCC2012010183	CIP-001-1a	R2.	During a Compliance Audit conducted from March 1 to April 5, 2011, NPCC determined that NAES, as a Generator Operator, had an issue with CIP-001-1a R2. Specifically, NAES Lockport failed to have any procedures directing the communication of information concerning sabotage reporting to appropriate parties in the Interconnection.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). When necessary, NAES Lockport has directed communications with other parties in the Interconnection through the use of the *Plant Managers Standing Orders (OP-101* . Therefore, should NAES Lockport need to direct communication of information concerning sabotage events to appropriate parties in the Interconnection, it would do so using the *Plant Managers Standing Orders (OP-101)* .	To mitigate this issue, NAES Lockport: 1) updated its sabotage reporting procedure to specifically address the communication of sabotage events to the Interconnection parties that need to be contacted; and 2) required the affected personnel to review the specific changes to the procedure.
Reliability*First* Corporation (Reliability*First)*	Michigan South Central Power Agency (MSCPA)	NCR00823	RFC2013012160	FAC-009-1	R1	From October 17, 2012 through November 9, 2012, Reliability*First* conducted a Compliance Audit. Reliability*First* identified that, as a Generator Owner, MSCPA had an issue with FAC-009-1, R1 because MSCPA did not use a common unit of measure on its facilities ratings sheet, which prevents a proper comparison of equipment elements to identify the most limiting element affecting output of the generator in the process of establishing Facility Ratings.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was a documentation issue. Despite not using common units, MSPCA had correctly determined that the total output of its generating unit was 50 MVA and that this output would not result in exceedences of the rating of any individual piece of equipment. In addition, MSCPA has a relatively small contribution to the BPS.	To mitigate this issue, MSCPA revised its Facility Ratings documentation to use a single unit of measure for FAC-009.
Reliability*First* Corporation (ReliabilityFirst)	Michigan South Central Power Agency (MSCPA)	NCR00823	RFC2013012161	PRC-001-1	R1	From October 17, 2012 through November 9, 2012, Reliability*First* conducted a Compliance Audit. Reliability*First* identified that, as a Generator Operator, MSCPA had an issue with PRC-001-1 R1 because MSCPA failed to provide evidence that its personnel were familiar with the purpose and limitations of protective system schemes applied in its area.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). MSCPA's operators were experienced in power plant operations, including the operation of protective system schemes applied in power plant operations. In addition, MSCPA has a relatively small contribution of to the BPS, consisting of one 55 MW generating unit that interconnects at 138 kV.	To mitigate this issue, MSCPA conducted training of its personnel to review the purpose and limitations of protective system schemes applied in its area.
Reliability*First* Corporation (Reliability*First)*	Michigan South Central Power Agency (MSCPA)	NCR00823	RFC2013012162	PRC-005-1	R1	From October 17, 2012 through November 9, 2012, Reliability*First* conducted a Compliance Audit. Reliability*First* identified that, as a Generator Owner, MSCPA had an issue with PRC-005-1, R1 because MSCPA failed to include a summary of maintenance and testing procedures in its Protection System maintenance and testing program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue was a documentation issue because MSCPA performed maintenance and testing in accordance with its program. In addition, MSCPA has a relatively small contribution to the BPS, consisting of one 55 MW generating unit that interconnects at 138 kV.	To mitigate this issue, MSCPA added a summary of maintenance and testing procedures to its Protection System maintenance and testing program.
Reliability*First* Corporation (Reliability*First*)	Metropolitan Edison Company (MetEd)	NCR00821	RFC2011001221	PRC-008-0	R2	During a Compliance Audit, conducted from October 4, 2011 through October 7, 2011, Reliability*First* determined that MetEd, as a Distribution Provider and Transmission Owner, had an issue with PRC-008-0 R2. Met Ed could not provide Under Frequency Load Shedding (UFLS) program results for three UFLS relays. MetEd could provide database maintenance and testing records that included the dates upon which it last maintained and tested its Fairview, Hokes, and Walker UFLS relays, but not the results of the maintenance and testing. Reliability*First* initially determined MetEd could not provide test results for four UFLS relays. However, one of the UFLS relays at issue had test results for 2009, but was missing test results for 2005. Reliability*First* determined that MetEd's missing 2005 test results did not indicate a possible violation of PRC-008-0 R2 as the testing occurred prior to the June 18, 2007, the date on which MetEd had to comply with PRC-008-0 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that this issue was a documentation issue. It was a documentation issue because MetEd could provide evidence demonstrating the most recent dates that each performed maintenance and testing on the three UFLS relays at issue, but not evidence of the results associated with the maintenance and testing. During the Compliance Audit, MetEd provided maintenance and testing dates as well as UFLS Program results for all other UFLS relays as requested by Reliability*First* . Additionally, the most recent maintenance and testing dates for the three UFLS relays at issue were within MetEd's five-year UFLS maintenance and testing interval.	To mitigate this issue, MetEd, where appropriate, disabled or completed maintenance and testing for the three UFLS relays and documented the UFLS Program results pursuant to PRC-008-0 R2 by December 31, 2012.

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)	Entergy	NCR01234	SERC2012010942	MOD-030-2	R2	On August 17, 2012, Entergy submitted a Self-Report to SERC stating that, as a Transmission Operator (TOP), it had an issue with MOD-030-2 R2 because it failed to incorporate a change to the Total Flowgate Capability (TFC) calculation within seven days of being notified of a change in the rating by the Transmission Owner (TO) that would affect the TFC of a Flowgate used in the Available Flowgate Capability (AFC) process. On May 25, 2012, one Flowgate on the Entergy transmission system was derated from 275 MW to 273 MW. The TO notified Entergy of the derate on the same day, but Entergy did not acknowledge receipt of the derate until June 11, 2012. Entergy did not incorporate the change to the TFC model until June 12, 2012, 18 calendar days after it was notified of the derate.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The derate was 2 MW, or 0.7%, of the Flowgate's capacity. In addition, the resulting TFC has not been approached during operation. Furthermore, the derate did not affect the steps that Entergy would take in the event the Rating had been exceeded.	To mitigate this issue, Entergy: 1) notified the TOP that a Flowgate rating change was necessary; 2) requested a change in the software used to calculate power flows for engineering analysis; 3) updated the AFC inputs database to include the correct rating of the Flowgate; 4) updated necessary documents to reflect the rating change of the Flowgate and sent the necessary documents to the TOP so they could be posted to the Open Access Same-Time Information System (OASIS); 5) received notification from the TOP that the updated documents had been posted to OASIS; 6) developed an AFC checklist to be used every time a rating change notification is received from configuration management to ensure that the AFC Flowgate will be identified and changed within the seven day window; 7) added the AFC checklist to its procedure for updating the transmission system topology in the daily and monthly powerflow models (transmission system topology procedure); and 8) trained applicable personnel on the transmission system topology procedure's AFC checklist. SERC has verified the completion of all mitigation activity.
SERC Reliability Corporation (SERC)	Cottonwood Energy Company LP (Cottonwood)	NCR01210	SERC2012011381	PRC-005-1	R2	On September 18, 2012, SERC sent Cottonwood an initial notice of a Compliance Audit scheduled for March 4, 2013 through March 8, 2013. On November 9, 2012, Cottonwood submitted a Self-Report to SERC stating that, as a Generator Owner, it had an issue with PRC-005-1 R2 because Cottonwood could not provide certain test documentation for 5 current transformers, 1 relay test date, and 5 missed communication system tests for 2 devices. SERC reviewed Cottonwood's Protection System procedures and a spreadsheet created by Cottonwood, which includes a complete inventory of the Cottonwood Protection System devices, defined intervals, and maintenance and test dates for the most current and previous dates listed for each Protection System device. Based on this review, SERC determined that Cottonwood tested 1 out of 62 protective relays (1.61%), 2 out of 2 associated communication system (ACS) devices (100%), 5 out of 404 voltage and current sensing devices (1.23%), and 1 out of 62 DC control devices (1.61%) outside of the defined intervals. In total, SERC determined that Cottonwood could not provide evidence that 9 out of 540 Protection System devices (1.67%) were compliant with PRC-005-1 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Cottonwood constantly monitors the communication channels of the ACS devices. In the event communications are lost, an alarm is generated and sent to the Cottonwood control room which is manned at all times, prompting personnel to investigate. Cottonwood's protective relays are wired such that a relay failure or trip activates alarms in the control center. Cottonwood subsequently tested all the Protection System devices with missed intervals and found that they were fully functional with no issues.	To mitigate this issue, Cottonwood: 1) reassigned the tracking and scheduling of all its Protection System devices; 2) developed a comprehensive list of all Protection System devices and associated test intervals and schedules; 3) tracked these test intervals with automatic reminders via the corporate tracking program, Intelex. This program tasks the responsible person on a quarterly basis to verify that the testing of all Protection System devices is completed in accordance with the intervals defined by its maintenance plan; and 4) tested all elements that were not tested according to scheduled intervals. SERC has verified the completion of all mitigation activities.
SERC Reliability Corporation (SERC)	Mackinaw Power, LLC (MACK)	NCR08082	SERC2012011014	PRC-005-1b	R2	On September 4, 2012, MACK submitted a Self-Report to SERC stating that, as a Generator Owner, it had an issue with PRC-005-1 R2 because it failed to perform the quarterly battery maintenance within the required interval. According to MACK, the preventive maintenance (PM) work order for the battery was generated, but plant personnel failed to initiate the applicable contractor schedule. The issue was discovered during a routine audit of open work orders. SERC reviewed the MACK Protection System procedures and the MACK-compiled spreadsheet, which included a complete inventory of the Protection System devices, the defined intervals, and the maintenance and test dates for the most current and the previous dates listed for each device. SERC determined that MACK tested 1 out of 117 protective relay devices (0.85%) and 4 out of 18 station batteries (22.22%) outside of the defined intervals. In total, 5 out of 435 Protection System devices (1.15%) were not in compliance with PRC-005-1 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Following the second quarter of 2012, maintenance and testing was completed for the missed batteries in accordance to the maintenance intervals. In addition, during the quarter that the scheduled maintenance and testing was not completed, MACK had performed all of the corresponding monthly maintenance as scheduled. Any deterioration in the performance or condition of the battery system should have been discovered during the monthly maintenance or the subsequent quarterly tests. The results of the tests confirm that the battery system should have performed its functions as designed if needed during that period. The transformer relay at issue was a microprocessor relay equipped with a self-diagnostic feature, which generates an alarm when the self-test results in an error due to relay failure. In addition, the transformer was being protected by a back up relay system consisting of analog and mechanical relays. The facilities are not critical to the BPS. A Notice of Confirmed Violation covering a violation of PRC-005-1 R1 for MACK was filed with FERC under NP09-42-000 on September 25, 2009. On October 23, 2009, FERC issued an order stating it would not engage in further review of the Notice of Penalty. SERC determined that the instant issue is appropriate for FFT treatment because it involves PRC-005-1 R2 and the prior violation involved PRC-005-1 R1. The present issue is separate and distinguished from the prior violation which occurred in 2008 and dealt with associated communication systems not being included in MACK's program even though MACK had and was testing associated communication systems.	To mitigate this issue, MACK: 1) changed the preventative maintenance process by assigning the tasks to plant personnel instead of using outside contracted services; and 2) designed and implemented a tool for the tracking maintenance and testing of protection equipment.
SERC Reliability Corporation (SERC)	Virginia Electric and Power Company (DP, LSE, TO) (VEPCO-Trans)	NCR01214	SERC2012011322	PRC-008-0	R2	On August 8, 2012, SERC sent VEPCO-Trans an initial notice of a Compliance Audit scheduled for February 4, 2013 through February 8, 2013. On October 24, 2012, VEPCO-Trans submitted a Self-Report with two issues to SERC stating that, as a Distribution Provider and Transmission Owner, it had an issue with PRC-008-0 R2 because six Under Frequency Load Shedding (UFLS) relays were tested outside of the defined interval. Furthermore, VEPCO-Trans could not produce the field record maintenance and testing documentation for six additional UFLS relays. In May 2012, VEPCO-Trans discovered that three substations containing two UFLS relays each were tested after the March 31, 2008 date specified in the Protection System Maintenance Program (PSMP). The PSMP required the UFLS relays to be tested annually. SERC staff learned that all six UFLS relays were tested by May 30, 2008. After these six UFLS relays were identified, VEPCO-Trans conducted a review and confirmed that all of the other UFLS relay maintenance and testing had been completed by the date stated in the PSMP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In 2008 VEPCO-Trans reported to SERC a system peak demand of 17,438 MW and a load shed value of 5,497 MW, which equals 31.52%. The three stations (six UFLS relays) tested beyond the compliance date totaled 230 MW. Excluding these three locations would have resulted in a load shed value of 5,266.3 MW (30.20%), which is still in excess of the 30% required by the regional criteria. The six UFLS relays were tested 60 days past the March 31, 2008 testing and maintenance date. When tested, the UFLS relays were found to be functioning properly and should have performed the intended function if called upon to do so. If these relays been called upon to operate due to a UFLS event and had not functioned properly, the 30% load shed value requirement would have still been met.	To mitigate this issue, VEPCO-Trans: 1) maintained and tested the six UFLS relays at issue; and 2) amended the PSMP's testing compliance date to reflect a floating maintenance and testing interval instead of the date-specific maintenance and testing date. This is consistent with other relays on VEPCO-Trans' transmission system.

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)	Entergy	NCR01234	SERC2012010276	PRC-011-0	R2	On May 17, 2012, Entergy submitted a Self-Report to SERC stating that, as a Transmission Owner and Distribution Provider, it had an issue with PRC-011-0 R2 because it did not have evidence that several metering points associated with its Undervoltage Load Shedding (UVLS) Protection System were properly maintained prior to the inclusion of the metering points in the UVLS program. On July 22, 2010, Entergy implemented a revised UVLS scheme. On that date, Entergy added five additional metering points to the program, making a total of 30 metered points. The five metering points had already been in service prior to being added to the UVLS scheme, but Entergy did not review the maintenance records to assure that the maintenance was current with that required for UVLS scheme metering point applications. Entergy discovered the missing documentation of maintenance and testing during an internal review of maintenance history which was performed in preparation for the 2012 PRC-011-0 Standard Self-Certification. Entergy cannot verify that the five metering points met the maintenance and testing criteria described in its UVLS program document until Entergy conducted scheduled maintenance on the metering points on May 6, 2011. The UVLS system associated with these five metering points protects a geographically limited area in East Texas with a peak load of 293 MW. With the addition of the five points, the UVLS system consists of 30 metering points, 22 batteries, 24 DC control circuits, 30 voltage transformers, and 11 current transformers, for a total of 117 UVLS devices. The five metering points that were not properly maintained constitute 4.27% of the UVLS devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Three of the five affected metering points are redundant with other metering points, so failure of those metering points should neither hinder nor cause the activation of UVLS. The other two metering points had low and high voltage alarms that would alert Entergy personnel in the event of a problem. In addition, the UVLS system protects a geographically limited area in East Texas with a peak load of 293 MW. Furthermore, Entergy subsequently checked the affected metering points and found that they were functioning normally.	To mitigate this issue, Entergy: 1) maintained the five identified metering points; 2) modified its UVLS plan revision process flowchart to provide clarity that voltage monitoring metering points, load monitoring metering points, and load-shed feeder breakers need to be addressed in the UVLS program; and 3) developed a lessons learned and reviewed it with the Entergy personnel responsible for UVLS items. SERC has verified the completion of all mitigation activity.
SERC Reliability Corporation (SERC)	Entergy	NCR01234	SERC2012010984	PRC-023-1	R1	On August 27, 2012, Entergy submitted a Self-Report to SERC stating that, as a Transmission Operator, it had an issue with PRC-023-1 R1 after discovering that a transformer overcurrent relay was set below 150% of the transformer's maximum nameplate rating. This issue was identified during a self-imposed review of PRC-023 setpoints. Setpoints for the transmission line relays had been reviewed prior to the enforcement date of PRC-023-1 (July 1, 2010), but the self-audit revealed that the review had overlooked the autotransformer protection relays. During the ensuing review of the 54 autotransformer relay setpoints, Entergy identified one relay used for protection of a 500 kV transformer that would operate at 149.66% of the highest transformer rating which is 0.34% below the required setpoint of 150%. Entergy reported that the time delay before tripping at 149.66% was 3.3 hours and the delay reduced to 6.1 minutes at 150%. The relay engineer responsible for the setpoint calculation allowed the result to be truncated and rounded to the nearest whole number rather than use Entergy's undocumented practice of using two decimal places.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The historical loading of this transformer has not exceeded 62% of the nameplate rating and the relay would not have operated at loads up to 149.65% of the transformer's Loadability Rating; thereby, providing opportunity for operator action. Additionally, a loading scenario that exceeds 149.65% for more than three continuous hours would also likely exceed 150% capacity, meaning the relay would likely have actuated even if the setpoint had been correct. Finally, if loading had stopped at 150%, the operators would still have had 6.1 minutes to respond.	To mitigate this issue, Entergy: 1) corrected the relay setting protecting the identified transformer to ensure settings correspond to 150% of the maximum nameplate rating or greater; 2) revised its relay settings procedure and calculations sheets to specify that design settings for overcurrent relays on autotransformers use a target of at least 151% of the maximum nameplate rating; 3) performed an extent of condition on Entergy's PRC-023-1 applicable transformers to ensure that overcurrent protection relays were set at or above 150% of the maximum nameplate rating; 4) implemented a process to ensure and document that PRC-023-1 applicable autotransformer overcurrent settings meet Requirement R1.10; and 5) implemented a process to document limiting factors for PRC-023-1 applicable autotransformer loading. SERC has verified the completion of all mitigation activity.
SERC Reliability Corporation (SERC)	Cottonwood Energy Company LP (Cottonwood)	NCR01210	SERC2013012003	VAR-002-1.1b	R3	On September 18, 2012, SERC sent Cottonwood an initial notice of a Compliance Audit scheduled for March 4, 2013 through March 8, 2013. On February 25, 2013, Cottonwood submitted a Self-Report to SERC stating that, as a Generator Operator, it had an issue with VAR-002-1.1b R3 because it failed to notify its Transmission Operator (TOP) of changes in the status of several power system stabilizers (PSSs) within 30 minutes. On January 9, 2013, while performing a required exciter verification data collection test on the exciter and PSS on Unit 2, Cottonwood personnel observed that the data results did not follow the typical model of a PSS signal trending normally. The control room operator turned the Unit 2 PSS off and back on in order to verify the data results. On January 10, 2013, Cottonwood calibrated the PSSs on Units 1, 3, and 4 by toggling the PSSs on and off, which resulted in status changes associated with each unit's PSS. Cottonwood did not notify the TOP during the test because Cottonwood was testing one generator at a time and Cottonwood had the other units online and running to manage its commitment to load. Cottonwood did not communicate these status changes in the PSSs to the TOP until January 11, 2013 at 3:35 p.m.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). When calibrating the PSSs, Cottonwood removed one unit's PSS from service at a time. Cottonwood had all eight generators at its facility operating while the calibration was performed over a two-day period. Therefore, Cottonwood had seven generators online with PSSs enabled while the four units' PSSs were individually calibrated, allowing Cottonwood to manage any changes to the BPS during the testing process. In addition, the longest time a single PSS was out of service was approximately 101 minutes.	To mitigate this issue, Cottonwood: 1) installed e-Notify software that works in conjunction with the plant monitoring software which allows configurable points with the capability to email recipients upon a state change of any given points within the plant monitoring software; 2) developed and posted a list of TOP personnel and system operator phone numbers in the plant control rooms; and 3) performed a review of the VAR-002 procedure with all plant personnel. SERC has verified the completion of all mitigation activities.
Southwest Power Pool Regional Entity (SPP RE)	Golden Spread Panhandle Wind Ranch, LLC (Golden Spread)	NCR11153	SPP2013011752	PRC-005-1	R1; R1.1; R1.2	On January 30, 2013, Golden Spread submitted a Self-Report stating that, as a Generator Owner, it had an issue with PRC-005-1 R1. Golden Spread did not specifically include maintenance and testing intervals or a summary of maintenance and testing procedures for its DC control circuitry in its documented Protection System maintenance and testing program (PSMTP).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. In 2011, during plant commissioning, Golden Spread tested all of its Protection System devices, including DC control circuitry to ensure that its Protection System devices were performing properly. Based on the testing performed in 2011, Golden Spread's DC control circuitry is only two years into the five-year test interval recommended in the NERC Protection System Maintenance Technical Reference for DC control circuitry.	To mitigate this issue, Golden Spread modified its PSMTP to include maintenance and testing intervals and a summary of maintenance and testing procedures for its DC control circuitry. SPP RE has verified the completion of all mitigation activity.

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)	Lea Power Partners, LLC (Lea Power)	NCR10301	SPP2012009183	PRC-005-1	R2	On January 17, 2012, Lea Power, as a Generator Owner, self-reported an issue with PRC-005-1 R2. In its Self-Report, Lea Power stated that it could not provide evidence that it had tested or maintained its three battery banks in 2009, nor could it provide evidence that it had tested or maintained its direct current (DC) control circuits since 2008. More recently, in 2011, Lea Power had failed to test its three station battery banks (100 %) and 92 of its 198 (46.5%) voltage and current transformers within the one and three years intervals, respectively, established in its Protection System maintenance and testing program. Additionally, Lea Power had not tested 28 of its 42 (66.6%) DC control circuits and 28 of its 42 (66.6%) protective relays within the three year interval established in its Protection System maintenance and testing program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The Protection Systems at issue belong to one generating facility (Hobbs), consisting of 550 MWs. Hobbs is a new generating unit, commissioned in 2008. All of the Hobbs Protection System devices were functionally tested during the acceptance testing performed at commissioning. Also, the intervals established in Lea Power's original Protection System maintenance and testing program (one year for station batteries; and three years for DC Control Circuits , protective relays, and instrument transformers) are conservative. The corresponding maximum allowable test intervals established in NERC's 2007 Protection System Maintenance technical reference are seven years for station batteries, five years for DC Control Circuits and protective relays, and seven years for instrument transformers. All of the implicated protection system devices were tested within the maximum intervals established in the NERC technical reference. In addition, many of the Hobbs' Protection System devices provide for trouble alarms to a control room manned 24x7. Problems with these Protection System devices would have resulted in operator intervention. The battery bank testing missed in 2009 occurred within one year of commissioning. As to the later battery bank intervals that were missed, testing was performed within one month of the due date. As for the missed intervals for instrument transformers, DC Control Circuits, and protective relays, testing was performed within one to five months of the due date.	Testing was completed on October 18, 2011 for all of the implicated Protection System devices. Manufacturer information, Model, Style information, and Serial Numbers (where applicable) were added to the Protection System Maintenance & Testing Program to assist in recordkeeping retrieval. This information was gathered during both a fall 2011 and spring 2012 outages. The Protection System Maintenance and Testing Program was revised with the updated information on April 3, 2012.
Southwest Power Pool Regional Entity (SPP RE)	Western Farmers Electric Cooperative (WFEC)	NCR01160	SPP2012011400	PRC-005-1	R1; R1.1; R1.2	During a November 8, 2012, Compliance Audit of WFEC, the SPP RE identified an issue with PRC-005-1 R1.1 and R1.2. WFEC, as a Generator Owner, did not include in its generation protection system maintenance and testing program (Program) the maintenance and testing interval, and the basis (R1.1) or a summary of maintenance and testing procedures (R1.2) for one of its associated communication systems, *i.e.* , a relay pilot wire system. WFEC had previously identified the relay pilot wire system for inclusion in its Program but had mistakenly relied on its engineering consultant's conclusion that the relay pilot wire system was not an associated communication system under the purview of the PRC-005 Protection System maintenance and testing Standard. The omission of the relay pilot wire system from the Program represented less than one percent (1 of 1,612) of the Protection System devices under WFEC's Program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although WFEC's Program did not include its relay pilot wire system, WFEC was continuously monitoring the system via a line current differential relay which provides alarms in the event of any loss of communications to a continuously manned plant control room. Additionally, the relays at each terminal of the relay pilot wire system were being tested in accordance with WFEC's Program. Finally, the relay pilot wire system at issue represented less than one percent of WFEC's Protection System devices. A Settlement Agreement covering three violations of PRC-005-1 R1, R1 and R2 for WFEC was filed with FERC in 2011. FERC issued an order stating it would not engage in further review of the Notice of Penalty. A Settlement Agreement covering one violation of PRC-005-1 R2 for WFEC was filed with FERC in 2012. FERC issued an order stating it would not engage in further review of the Notice of Penalty. While WFEC's violation history contains prior violations of PRC-005-1 R1.1 and 1.2, which are similar to the present issue, SPP RE chose FFT treatment for the present issue for the following reasons: 1) the relay pilot wire system was being continuously monitored; 2) WFEC made a good faith effort to include the relay pilot wire system in its Program but mistakenly omitted it; 3) WFEC notified SPP RE prior to the Audit that it had discovered inconsistencies in its consultant's identification of WFEC's PRC-005-1 inventory and was taking steps to discover and remediate all issues; 4) WFEC's cooperation and efforts to improve its compliance culture; and 5) the minimal risk to the BPS posed by this issue. Additionally, the prior two violations of PRC-005-1 R2 are not relevant to the particular set of facts and circumstances in this issue, and do not hinder this issue from being processed as an FFT candidate.	WFEC amended its Program to include the relay pilot wire system, the system's maintenance and testing interval and its basis, and a summary of the procedure for performing maintenance and testing on the system. SPP RE verified that all mitigating activities were completed.
Texas Reliability Entity, Inc. (Texas RE)	Oncor Electric Delivery Company LLC (Oncor)	NCR04109	TRE2012011183	FAC-009-1	R1	On August 31, 2012, Oncor, as a Transmission Owner, submitted a Self-Certification identifying an issue with Reliability Standard FAC-009-1 R1. Oncor did not establish facility ratings consistent with Oncor's facility ratings methodology (FRM). Specifically, the 15-mintue ratings for 20 autotransformers were inaccurate. Also, one of these 20 autotransformers, and an additional five autotransformers had faulty cooling equipment, which resulted in inaccurate normal ratings. Both instances constituted inaccurate ratings as defined within Oncor's FRM. The issue period is from June 28, 2007, Oncor's registration date, through August 10, 2012, when the settings were reset.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). The 15-minute ratings were never utilized during the pendency of this issue. In addition, a review of loading levels for this time period for the autotransformers with faulty cooling equipment indicated that load levels were well below the new normal ratings. The inaccurate ratings resulted in incorrect relay overcurrent protection, which posed a possible risk to the protection of the autotransformers but minimal risk to the BPS.	To mitigate this issue, Oncor: 1) reset autotransformer relay settings where engineering studies had been completed; 2) temporarily disabled redundant autotransformer relay, provided protection was not compromised, until new relay settings could be reviewed and installed. All of these relays have been put back in service; 3) initiated a change to autotransformer facility ratings based on existing autotransformer relay setting; and 4) initiated a change to autotransformer facility ratings based on the recalculation of the autotransformer cooling equipment.
Texas Reliability Entity, Inc. (Texas RE)	Oncor Electric Delivery Company LLC (Oncor)	NCR04109	TRE201100459	PRC-005-1	R2; R2.1	On August 31, 2011, Oncor, as a Transmission Owner and Distribution Provider, submitted a Self-Report to Texas RE, citing non-compliance with Reliability Standard PRC-005-1 R2. Oncor tested its Protection Systems, which are divided into panels, at its different locations. Each panel could include one or more of five Protection Systems. Oncor missed testing on 4 panels, with 4 out of 5 devices on each panel not being tested. One of these 4 panels missed battery testing on the fifth device. From November 30, 2010, thorough August 30, 2011, Oncor missed 4 out of 1,762 panels (0.23%) for testing according to its defined intervals. Oncor identified the following reasons to be the cause of the issue: 1) a work order which was created to test the four Protection Systems was incorrectly closed prior to the work being performed. A new work order was created, but the date did not match the maintenance due date; and 2) a battery was erroneously classified as a non-Oncor asset and therefore was not tested by Oncor in accordance with Oncor's maintenance and testing program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the 4 reported panels that were not tested account for only 0.23% of Oncor's total of 1,762 relay Protection Systems. Additionally, batteries were not tested at one of the four reported panels but were tested at the other three panels. A Settlement Agreement covering a violation of Reliability Standard PRC-005-1 R2 for Oncor was filed with FERC under NP12-26-000 on April 30, 2012. On May 30, 2012, FERC issued an order stating it would not engage in further review of the Notice of Penalty. Texas RE determined that the instant issue is appropriate for a FFT treatment because the prior violation was related to Oncor's database not being populated correctly. Unlike the prior violation, the instant issue is related to a work order and an ownership classification type of noncompliance.	To Mitigate this issue, Oncor: 1) reviewed the Protection Systems in shared facilities to re-confirm ownership classification and maintenance and testing are properly prioritized and scheduled; 2) instituted a validation procedure to perform periodic assessments to ensure no unexpected intervals have been generated as a result of data entry activity; 3) reviewed and enhanced existing processes for work order data entry and completion; 4) evaluated assets to validate last maintenance test date and create on-going validation tool; 5) developed a training program, training materials, and schedules required to implement the specified process improvements; and 6) reported and documented progress and deliverables, including new procedures, status updates, and completion reports as appropriate. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	USACE - Tulsa District (USACE)	NCR04156	TRE2012009734	MOD-012-0	R2	On January 25, 2012, USACE submitted a Self-Report to Texas RE indicating that as a Generator Owner, it had an issue with MOD-012-0 R2. USACE did not provide dynamics system modeling data to its Regional Reliability Organization (RRO), as required by the Standard. In particular, on February 28, 2008, USACE received a dynamics data request from its third-party contractor who had been delegated certain activities related to data submittals. On March 13, 2008, USACE submitted the requested data to the third-party contractor with an expectation that the third-party contractor would forward the data to the RRO. However, during a 2012 internal review, USACE could not find any evidence that the data had been provided to the RRO in 2008. USACE submitted a Self-Report in January 2012, and in December 2012 it submitted the data to the RRO. The duration of this issue was from March 15, 2008, when the data request should have been answered, through December 13, 2012, when the data was supplied to the RRO.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Without the submitted data, the RRO would have relied on simulated data for its analysis, which is a customary practice when data is not readily available. Texas RE determined that the simulation data is very accurate when compared with the modeling data. The data at issue was for current information at the plant, and in the last five years, ERCOT has asked for this data twice. Finally, the nameplate rating of the facility is approximately 80 MW, which further reduced the risk to the BPS.	To mitigate this issue, USACE submitted the revised dynamics data to the RRO via e-mail on December 13, 2012. Texas RE has verified the completion of all mitigation activities.
Western Electricity Coordinating Council (WECC)	Puget Sound Energy, Inc. (PSE)	NCR05344	WECC2013011932	FAC-501-WECC-1	R2	On February 15, 2013, PSE submitted a Self-Certification to WECC stating that, as a Transmission Owner that maintains a transmission path in the most current table titled, "Major WECC Transfer Paths in the Bulk Electric System," it had an issue with FAC-501-WECC-1 R2. PSE stated that it failed to include item 4.b of Attachment 1-FAC-501-WECC-1, "Station Maintenance Details: Contamination Control" in its Transmission Maintenance and Inspection Plan (TMIP). Specifically, PSE stated that it has an internal procedure titled, TL0002: Contamination Control and Insulator Washing (TL0002) that has been included in the TMIP since January 3, 2005 and details PSE's approach to both station and line insulator contamination control, but that this procedure was referenced in the Transmission Line Maintenance section and did not clearly apply to station maintenance, as required by FAC-501-WECC-1 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risk posed by this failure was reduced as a result of existing protections in place during the pendency of the issue. PSE does have an internal document that addressed contamination controls. Specifically, PSE's internal document TL0002 detailed maintenance intervals and evaluation criteria for substation operations, and this document was available to all employees for the duration of the issue. Furthermore, per this internal procedure, PSE performs contamination control on an as-needed basis.	To mitigate this issue PSE updated its TMIP to include a thorough explanation of its policy for contamination control for both station and line insulators. The updated TMIP also includes reference to PSE's existing contamination control procedure. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Western Area Power Administration - Sierra Nevada Region (WASN)	NCR05465	WECC200801236	PRC-005-1	R2	On December 18, 2008, WASN submitted a Self-Report to WECC stating that, as a Transmission Owner it had an issue with PRC-005-1 R2. Specifically, WASN reported that it had failed to complete maintenance and testing of its DC control circuitry at its Shasta substation (one of 15 WASN substations) within the defined intervals of its Protection System maintenance and testing program. WASN reported that testing was to be completed on December 5, 2008, but, due to several equipment failures, it was unable to complete testing on time. WASN reported that testing was actually completed on December 20, 2008.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). WASN performed maintenance and testing on its other Protection System devices at its Shasta substation. Additionally, WASN began maintenance and testing prior to the expiration of the defined interval and only failed to complete testing due to equipment failure. Once WASN realized that testing would not be completed within the defined interval it took immediate steps to resolve the issues preventing testing. Once testing was possible, testing was completed within two weeks of the required date. Further, not only did WASN maintain and test all other protection systems at its Shasta substation within the intervals defined in its program, but WASN also maintained and tested its Protection System devices in accordance with WASN's defined intervals for the remainder of WASN's 15 substations. A Settlement Agreement covering a violation of PRC-005-1 R2 for WASN was filed with FERC in the Omnibus filing under NP10-2-000 on October 14, 2009. The instant issue was appropriate for Find, Fix, Track and Report processing because the prior violation also posed a minimal risk to the reliability of the BPS, included only one substation, and testing was late by a limited number of days.	To mitigate this issue, WASN completed annual DC system maintenance at the Shasta Substation. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Hatchet Ridge Wind, LLC (HRWL)	NCR11039	WECC2013012016	VAR-002-1.1b	R1	On February 28, 2013, HRWL submitted a Self-Certification to WECC stating that, as a Generator Operator, it had an issue with VAR-002-1.1b R1. Specifically, HRWL reported that its capacitor banks, acting as a part of its automatic voltage control scheme, were operating in manual mode instead of automatic mode as required by the Standard. HRWL reported that its capacitor banks had been operating in manual mode because a relay that controlled its capacitor bank switches was operating in manual mode instead of automatic mode. HRWL reported that, after commissioning, it received indication that the relay controlling the capacitor bank switches was operating in manual mode. HRWL reported that it ignored the indication believing the indication was incorrect. In February of 2013, HRWL reported that it hired a third-party contractor to test the indicator light and, at the time of testing, HRWL was informed that the indicator was correct and that the relay had been operating in manual mode, causing HRWL to operate its generators in a mode other than automatic voltage control mode (with the automatic voltage regulator controlling voltage). HRWL operated in such a mode since it commissioned its units. HRWL reported that it immediately changed the relay controlling its capacitor banks to automatic mode, which in turn, allowed its capacitor banks to operate automatic mode, and informed its Transmission Operator (TOP) of the status change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. HRWL's voltage control scheme includes a Load Tap Changer (LTC) located at its point of interconnection with its TOP. The LTC operates independently of the capacitor banks and helps to regulate voltage fluctuations within predefined levels to help limit the potential risks associated with voltage fluctuations. HRWL is a small wind generation facility that produces 101 MW and its load is not considered a base load. HRWL operates at an annual capacity factor of around 20 percent per year.	To mitigate this issue, HRWL: 1) changed the relay controlling its capacitor bank switches from manual mode to automatic mode and notified its TOP of the change within 30 minutes; 2) took preventative steps including adjusting its voltage control setup; developing and implementing improved functional voltage monitoring and control procedures; reviewing, verifying and implementing additional telemetry; and training its personnel on new voltage control procedures.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1) Clewiston, City of (CLE)	NCRXXXXX	FRCC2013011753	CIP-003-3	R2.2	FRCC_URE1 submitted a Self-Report to FRCC stating that it had an issue with CIP-003-3 R2.2 because it failed to document the appointment of a new senior manager within 30 calendar days of the effective date after the resignation and formal removal of the previous senior manager. The issue was discovered during a self-audit by the compliance officer. The new senior manager was designated and the internal control policy document was updated eight days later.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. FRCC_URE1 does not own any Critical Assets or Critical Cyber Assets, and the issue duration was a short period of time. Furthermore, the acting senior manager during the issue period was the compliance officer who had been on staff for three years and was trained on the CIP standards. FRCC_URE1 is also a small entity.	To mitigate this issue FRCC_URE1: 1) assigned the new CIP senior manager; 2) drafted the CIP-003-3 senior manager appointment internal control policy; 3) presented the CIP-003-3 senior manager internal control policy to executives for review; 4) implemented the CIP-003-3 senior manager appointment internal control policy.
Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC2011008537	CIP-006-1	R1; R1.1	FRCC conducted a Spot Check and determined that FRCC_URE2 had an issue with CIP-006-1 R1.1. Specifically, FRCC_URE2 failed to ensure that all Cyber Assets were within an identified Physical Security Perimeter (PSP). Specifically, the ethernet wiring that is an integral part of the network and thus a Critical Cyber Asset (CCA) was not protected inside a PSP and appropriate physical access control was not provided.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was reduced because the only exposed portion of the cabling was for a short length on either side as it exited the buildings housing the PSPs. In addition, the affected buildings are within secured facilities for which physical access is controlled by security guards along with video monitoring.	To mitigate this issue, FRCC_URE2 moved the access point for the Electronic Security Perimeter (ESP) from the main building to the safe room. This made the entire ESP and the access point within the same physical cage. FRCC has verified the completion of the mitigation activity.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012009744	CIP-004-3	R2; R2.1	NPCC_URE1 submitted a Self-Report to NPCC stating that it had an issue with CIP-004-3 R2.1. NPCC_URE1's site security processed a completed physical access request form for a building and grounds employee with access to Critical Cyber Assets (CCAs). The request form provided a training date which was the date the employee took NPCC_URE1's 2011 NERC Reliability Standards awareness training. The employee had not taken NPCC_URE1's 2011 mandatory cyber security training, which is required prior to granting unescorted physical access to CCAs and is updated and provided annually to individuals with such access. The error in granting access to the Physical Security Perimeter (PSP) that contained CCAs was discovered and the employee's authorized physical access was immediately revoked by site security.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the employee had not completed the 2011 mandatory cybersecurity training, the employee had completed this training in 2010. Also, the employee was only granted access to a single PSP and review by NPCC_URE1 security confirmed that the employee had not entered the PSP during the eight-day period he was granted access.	To mitigate this issue, NPCC_URE1: 1) conducted a review of all authorized access request forms to ensure no authorized access had been granted to other employees who had not taken the 2011 mandatory cyber security training; based on completion of the 2011 NERC Reliability Standards awareness training, and revoked immediately in such instances; and 2) issued a guidance statement to staff reaffirming the requirements of CIP-004 for applicable training that must be completed for unescorted physical access to CCAs, along with a PowerPoint training program for them to review.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008006	CIP-002-1	R3	NPCC_URE2 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-1 R3. NPCC_URE2 did not update its list of Critical Cyber Assets (CCAs) when new devices were added within an Electronic Security Perimeter (ESP). During a four month time span, NPCC_URE2 converted remote network terminal units (NTUs) from serial communication protocol to an internet protocol (IP) routable protocol. During this process, a network switch was also added to the communication path. The NTUs were added to the CCA inventory but the network switches were not added.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The IT engineer who maintains all the network switches treated the devices as if they were all CCAs. In addition, these network switches were behind a firewall appliance that was an electronic access point for the substation ESP.	To mitigate this issue, NPCC_URE2: 1) had cybersecurity team personnel assess and inventory each CCA and validate connection diagrams; 2) moved the Cyber Asset inventory list from the spreadsheet to the change management database; 3) issued an inventory list for senior manager to approve; 4) discussed with cybersecurity team the importance of listing all assets to be connected to an ESP on the change management ticket and to update the inventory of Cyber Assets at the time of installation or connection within the ESP; and 5) validated that the cybersecurity team understood the importance of listing and updating CCAs by repeating the mitigating actions above in January 2012 and requested the security team members sign an attendance sheet listing all dates.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008335	CIP-007-1	R4	NPCC_URE3 submitted a Self-Report to NPCC stating that it had an issue with CIP-007-1 R4. Specifically, the operating systems on a number of Cyber Asset devices did not have anti-virus and anti-malware tools installed. NPCC_URE3 failed to submit a Technical Feasibility Exception (TFE) request for the devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue reside within a Physical Security Perimeter and an Electronic Security Perimeter. In addition, the incident response plan will notify support personnel to take action in the event a device is compromised and the facility IT contact will interface with the corporate cyber incident response team providing assistance with communication and remediation. Furthermore, network isolation prevents exposure of devices to un-trusted networks, including the Internet and business network.	To mitigate this issue, NPCC_URE3 submitted an open-ended TFE which was accepted and approved by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2012010460	CIP-007-1	R3	NPCC_URE3 submitted a Self-Report to NPCC stating that it had an issue with CIP-007-1 R3. Specifically, it could not implement a security patch management program for a number of personal computers. NPCC_URE3 failed to submit a Technical Feasibility Exception (TFE) request for the personal computers.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue reside within a Physical Security Perimeter and an Electronic Security Perimeter. In addition, the incident response plan will notify support personnel to take action in the event a device is compromised and the facility IT contact will interface with the corporate cyber incident response team providing assistance with communication and remediation. Furthermore, network isolation prevents exposure of devices to untrusted networks, including the Internet and business network.	To mitigate this issue, NPCC_URE3 submitted an open-ended TFE which was accepted and approved by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011008441	CIP-007-1	R4	NPCC_URE4 submitted a Self-Report to NPCC stating that it had an issue with CIP-007-1 R4. Specifically, the operating systems on a number of devices did not have anti-virus and anti-malware tools installed. NPCC_URE4 failed to submit Technical Feasibility Exception (TFE) request for these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue reside within a Physical Security Perimeter and an Electronic Security Perimeter. In addition, the incident response plan will notify support personnel to take action in the event a device is compromised and the facility IT contact will interface with the corporate cyber incident response team providing assistance with communication and remediation. Furthermore, network isolation prevents exposure of devices to untrusted networks, including the Internet and business network.	To mitigate this issue, NPCC_URE4 submitted an open-ended TFE which was accepted and approved by NPCC.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2012010425	CIP-007-1	R6	NPCC_URE4 submitted a Self-Report to NPCC stating that it had an issue with CIP-007-1 R6. Specifically, a number of devices were not capable of generating internal logs of system events including security and authentication-related incidents. NPCC_URE4 failed to submit Technical Feasibility Exception (TFE) requests for these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue reside within a Physical Security Perimeter and an Electronic Security Perimeter. In addition, the incident response plan will notify support personnel to take action in the event a device is compromised and the facility IT contact will interface with the corporate cyber incident response team providing assistance with communication and remediation. Furthermore, network isolation prevents exposure of devices to untrusted networks, including the Internet and business network.	To mitigate this issue, NPCC_URE4 submitted an open-ended TFE which was accepted and approved by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2013012291	CIP-007-1	R5; R5.3	During an on-site Compliance Audit, NPCC discovered that NPCC_URE4 had an issue with CIP-007-1 R5.3. Specifically, a number of devices did not have technical controls for password length, character complexity, or password change frequency. NPCC_URE4 failed to submit Technical Feasibility Exception (TFE) requests for these device.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue are protected by the Electronic Security Perimeter and Physical Security Perimeter. Additionally, personnel risk assessments and training ensure that only vetted personnel have access to these devices. Furthermore, proprietary machine language for instructions inhibits plug-in and control by a potential hacker.	To mitigate this issue, NPCC_URE4 submitted an open-ended TFE which was accepted and approved by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2012010465	CIP-007-1	R6	NPCC_URE5 submitted a Self-Report to NPCC stating that it had an issue with CIP-007-1 R6. Specifically, a number of devices were not capable of generating internal logs of system events including security and authentication-related incidents. NPCC_URE5 failed to submit Technical Feasibility Exception (TFE) requests for these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue reside within a Physical Security Perimeter and an Electronic Security Perimeter. In addition, the incident response plan will notify support personnel to take action in the event a device is compromised and the facility IT contact will interface with the corporate cyber incident response team providing assistance with communication and remediation. Furthermore, network isolation prevents exposure of devices to untrusted networks, including the Internet and business network.	To mitigate this issue, NPCC_URE5 submitted an open-ended TFE which was accepted and approved by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6) Noble Altona Windpark, LLC	NCRXXXXX	NPCC2012011601	CIP-002-3	R1; R1.1	NPCC_URE6 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE6 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE6 completed a documented RBAM. NPCC_URE6 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE6 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6) Noble Altona Windpark, LLC	NCRXXXXX	NPCC2012011602	CIP-002-3	R2	NPCC_URE6 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R2. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE6 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE6 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE6 completed a documented RBAM. NPCC_URE6 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE6 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6) Noble Altona Windpark, LLC	NCRXXXXX	NPCC2012011604	CIP-002-3	R4	NPCC_URE6 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE6 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE6 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE6 completed a documented RBAM. NPCC_URE6 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE6 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 7 (NPCC_URE7) Noble Bliss Windpark, LLC	NCRXXXXX	NPCC2012011605	CIP-002-3	R1; R1.1	NPCC_URE7 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE7 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE7 completed a documented RBAM. NPCC_URE7 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE7 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 7 (NPCC_URE7) Noble Bliss Windpark, LLC	NCRXXXXX	NPCC2012011606	CIP-002-3	R2	NPCC_URE7 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE7 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE7 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE7 completed a documented RBAM. NPCC_URE7 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE7 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 7 (NPCC_URE7) Noble Bliss Windpark, LLC	NCRXXXXX	NPCC2012011608	CIP-002-3	R4	NPCC_URE7 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE7 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE7 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE7 completed a documented RBAM. NPCC_URE7 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE7 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 8 (NPCC_URE8) Noble Chateaugay Windpark, LLC	NCRXXXXX	NPCC2012011609	CIP-002-3	R1, R1.1	NPCC_URE8 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE8 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE8 completed a documented RBAM. NPCC_URE8 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE8 completed and documented a RBAM for Critical Assets.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 8 (NPCC_URE8) Noble Chateauguay Windpark, LLC	NCRXXXXX	NPCC2012011610	CIP-002-3	R2	NPCC_URE8 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. NPCC_URE8 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE8 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE8 completed a documented RBAM. NPCC_URE8 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE8 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 8 (NPCC_URE8) Noble Chateauguay Windpark, LLC	NCRXXXXX	NPCC2012011612	CIP-002-3	R4	NPCC_URE8 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE8 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE8 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE8 completed a documented RBAM. NPCC_URE8 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE8 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 9 (NPCC_URE9) Noble Clinton Windpark, LLC	NCRXXXXX	NPCC2012011621	CIP-002-3	R1, R1.1	NPCC_URE9 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE9 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE9 completed a documented RBAM. NPCC_URE9 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE9 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 9 (NPCC_URE9) Noble Clinton Windpark, LLC	NCRXXXXX	NPCC2012011622	CIP-002-3	R2	NPCC_URE9 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE9 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE9 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE9 completed a documented RBAM. NPCC_URE9 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE9 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 9 (NPCC_URE9) Noble Clinton Windpark, LLC	NCRXXXXX	NPCC2012011624	CIP-002-3	R4	NPCC_URE9 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE9 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE9 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE9 completed a documented RBAM. NPCC_URE9 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE9 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 10 (NPCC_URE10) Noble Ellenburg Windpark, LLC	NCRXXXXX	NPCC2012011613	CIP-002-3	R1; R1.1	NPCC_URE10 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE10 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE10 completed a documented RBAM. NPCC_URE10 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE10 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 10 (NPCC_URE10) Noble Ellenburg Windpark, LLC	NCRXXXXX	NPCC2012011614	CIP-002-3	R2	NPCC_URE10 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE10 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE10 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE10 completed a documented RBAM. NPCC_URE10 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE10 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 10 (NPCC_URE10) Noble Ellenburg Windpark, LLC	NCRXXXXX	NPCC2012011616	CIP-002-3	R4	NPCC_URE10 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE10 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE10 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE10 completed a documented RBAM. NPCC_URE10 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE10 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 11 (NPCC_URE11) Noble Wethersfield Windpark, LLC	NCRXXXXX	NPCC2012011617	CIP-002-3	R1, R1.1	NPCC_URE11 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE11 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE11 completed a documented RBAM. NPCC_URE11 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE11 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 11 (NPCC_URE11) Noble Wethersfield Windpark, LLC	NCRXXXXX	NPCC2012011618	CIP-002-3	R2	NPCC_URE11 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE11 did not develop a list of its identified Critical Assets through an annual application of the RBAM as required by CIP-002-3 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE11 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE11 completed a documented RBAM. NPCC_URE11 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE11 completed and documented a RBAM for Critical Assets.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 11 (NPCC_URE11) Noble Wethersfield Windpark, LLC	NCRXXXXX	NPCC2012011620	CIP-002-3	R4	NPCC_URE11 submitted a Self-Report to NPCC stating that it had an issue with CIP-002-3 R1. Prior to 2012, IT personnel and previous NERC responsible personnel failed to document its risk-based assessment methodology (RBAM) for Critical Assets. Therefore, NPCC_URE11 did not have annual approval of the RBAM by senior management or delegate(s) pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NPCC_URE11 conducted the required assessments to determine whether it had Critical Assets since it was registered, but failed to document its findings. Upon realization, NPCC_URE11 completed a documented RBAM. NPCC_URE11 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-3.	To mitigate this issue, NPCC_URE11 completed and documented a RBAM for Critical Assets.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1) CMS Generation Michigan Power, L.L.C. (CMSMP)	NCRXXXXX	RFC2013012124	CIP-003-1	R2; R2.1	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-003-1 R2.1. RFC_URE1 did not have a separate specific document that identified the CIP senior manager by name, title, and date of designation for one year. A RFC_URE1 senior manager was acting as the senior manager delegate in the duration of the issue, and that senior manager approved the Critical Asset assessments and the lists of Critical Assets and Critical Cyber Assets. While the former CIP senior manager is no longer the CIP senior manager, the individual maintains a position with RFC_URE1 as the director of technical operations for an affiliate company.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was limited to documentation, was of a short duration, and concerned an individual that remains a trusted employee of an affiliate company.	To mitigate this issue, RFC_URE1: 1) conducted a review of its CIP procedure; 2) maintains a current and accurate designation of senior manager letter stored in the electronic document management program for document retention; 3) created a task activity in the electronic data tracking system that will generate an annual reminder to review senior manager assignments; and 4) utilizes a managerial transition checklist when a change in senior management occurs within 30 days to assign a new senior manager.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2013011664	CIP-006-3c	R2.2	RFC_URE2 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-004-3 R3. Reliability*First* subsequently determined that the facts and circumstances of this Self-Report constituted an issue of CIP-006-3c R2.2 because on RFC_URE2 mistakenly granted authorized cyber access to Physical Access Control System servers, Cyber Assets that authorize and/or log access to the Physical Security Perimeter, to the supervisor that approved the access request instead of the employee who required such access. RFC_URE2 discovered the issue through a routine, periodic user access review, and the next day revoked the supervisor's access.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individual at issue is a long-time employee. RFC_URE2 provides separate access grants to the operating system, database, and application for its assets. In order to modify, view physical access control data, application configuration, and or database elements, RFC_URE2 must grant either the database level access or application level access. Operating system level access does not afford change/view privilege. RFC_URE2 confirmed that the supervisor had not logged into the servers during the time period of the issue, and the supervisor did not attempt such access.	To mitigate this issue, RFC_URE2: 1) revoked the supervisor's access and reviewed the security logs from the servers to determine whether the supervisor had accessed the servers; 2) confirmed that the supervisor had not logged into the servers during the time period of the issue, and the supervisor did not attempt such access; and 3) defined and implemented a new access role that is limited to the Physical Access Control System servers and changed the business unit responsible for provisioning access to the servers to the information security – identity and access management group.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100872	CIP-005-1	R1; R1.4; R1.6	RFC_URE3 self-certified to Reliability*First* that it had an issue with CIP-005-1 R1. RFC_URE3 had not identified or protected several non-critical Cyber Assets located within the Electronic Security Perimeter (ESP) pursuant to CIP-005-1 R1.4. The non-critical Cyber Assets at issue consist of non-essential devices associated with plant monitoring and printers or print servers. RFC_URE3 also did not maintain documentation for certain Critical Cyber Assets (CCAs) and non-critical Cyber Assets pursuant to CIP-005-1 R1.6. First, RFC_URE3 did not document each interconnected CCA and non-critical Cyber Asset located in ESPs on its ESP network diagrams. Second, FE Genco did not timely submit Technical Feasibility Exception (TFE) requests for several assets as required by Appendix 4D to NERC's Rules of Procedure. The non-critical Cyber Assets and CCAs at issue with CIP-005-1 R1.6 consist of non-critical Cyber Assets associated with plant monitoring CCAs associated with plant monitoring, a GPS clock, and a printer.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. First, firewalls surrounding the non-critical Cyber Assets at issue were programmed to deny general interactive access to the non-critical Cyber Assets. Second, RFC_URE3's parent company's information technology group monitored and alarmed the firewalls surrounding the non-critical Cyber Assets at issue for authorized and unauthorized access attempts. Third, the non-critical Cyber Assets and CCAs at issue are not located within a system control center, but rather within generation plant Physical Security Perimeters (PSPs) accessible only by escorted individuals or those individuals with valid personnel risk assessments and prior CIP training. Fourth, RFC_URE3 afforded the non-critical Cyber Assets the protective measures specified in the applicable requirements of CIP-003, with the exception of R6, CIP-004, CIP-006, and CIP-008. Fifth, the issue with CIP-005-1 R1.6 is a documentation issue. During the duration of the issue, RFC_URE3 provided the required protections to the CCAs and non-critical Cyber Assets that it had not documented on its ESP network diagrams. Additionally, for the duration of the issue, RFC_URE3 provided the CCAs with the protections described in its TFE requests. The TFE requests addressed CIP-007 requirements. The protections described in the TFE requests included: containing the devices within an ESP and a six-wall PSP that are only accessible by personnel trained and subject to background checks; installing anti-virus software, where possible, to protect against malware; two factor authentication; and port mapping. Reliability*First* accepted and approved each of the TFE requests for the CCAs at issue.	To mitigate this issue, RFC_URE3: 1) identified and protected all non-critical Cyber Assets located within the ESP pursuant to CIP-005-1, R1.4; and 2) maintained documentation for all CCAs and non-critical CCAs pursuant to CIP-005-1 R1.6. Reliability*First* verified that RFC_URE3 completed all necessary mitigating activities.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2013012070	CIP-006-3c	R1; R1.4	RFC_URE4 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-006-3c R1.4. An employee used a key, intended for emergency use only, to enter a physical security perimeter (PSP) for which the employee was not authorized. The employee's supervisor had directed the employee to enter the PSP to switch a line into service in anticipation of the arrival of a major weather event. By using the key to enter the PSP, the employee bypassed normal access controls and actuated an alarm. Security personnel investigated the alarm and required the employee to leave the PSP when they determined the employee was not authorized to enter the PSP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The employee at issue was a long time RFC_URE4 parent company employee with a valid personnel risk assessment (PRA) at the time of the issue. Additionally, RFC_URE4's security personnel detected the improper entry into the PSP and escorted the employee out of the PSP within 15 minutes of entry. Finally, the human performance error which caused this issue was precipitated by the impending arrival of the major weather event. In order to expedite RFC_URE4's switching of the line into service prior to the arrival of the weather event, the employee's supervisor selected the next available individual without validating the employee's CIP authorization to that specific substation.	To mitigate this issue, RFC_URE4: 1) conducted CIP training and granted access to enter substation PSPs for the employee at issue; and 2) conducted CIP training, completed PRAs and granted access to enter substation PSPs for other employees who perform similar duties as the employee at issue.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2012010355	CIP-008-3	R1	RFC_URE5 self-certified to Reliability*First* that it had an issue with CIP-008-3 R1. While RFC_URE5 had a procedure for updating its Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE5 did not update its Cyber Response Plans within 30 calendar days on several occasions. Specifically, RFC_URE5 failed to change referenced procedure versions or designation numbers in their Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE5 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE5: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated RFC_URE5's Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE5 removed unnecessary document references within the Cyber Response Plan to reduce any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE5 to update the Cyber Response Plan following minor changes to referenced documents.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC2013012074	CIP-004-3a	R3	RFC_URE6 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-004-3a. RFC_URE6 granted a vendor without a valid personnel risk assessment (PRA) cyber access to a Critical Cyber Asset (CCA). RFC_URE6 held an information and training program for an Electronic Access Control and Monitoring System. An authorized RFC_URE6 employee logged into a shared account and then turned navigation over to the vendor so the vendor could perform a demonstration. The vendor did not have a valid PRA. For one hour, the vendor navigated in the production environment of the security information and event management application, a CCA, through the shared account. As a result, RFC_URE6 granted the vendor authorized cyber access without conducting a PRA.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individual at issue was an employee from a trusted vendor with whom RFC_URE6 has confidentiality and non-disclosure agreements in place. The demonstration was done for RFC_URE6 employees with authorized cyber access and a business need to know. These employees had appropriate training and valid PRAs.	To mitigate this issue, RFC_URE6: 1) conducted a training session for the management, which included RFC_URE6's current CIP access and PRA approval process as well as the NERC project 2009-26 Interpretation of CIP-004-3; and 2) performed a review of all vendors' PRA documentation and non-disclosure agreements.

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2012011426	CIP-002-3	R2	Five months after receiving an initial notice of a Compliance Audit, SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-002-3 R2 because it did not have evidence of the annual application of the risked-based assessment methodology (RBAM) to develop a list of its identified Critical Assets for one year. SERC_URE1 had applied its RBAM annually before and after the missed year to develop its list of identified Critical Assets. SERC_URE1 determined that it had no Critical Assets in each of those years. SERC confirmed that SERC_URE1 could not provide evidence it applied its RBAM to develop its list of Critical Assets for one year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1 had applied its RBAM annually before and after the missed year and did not identify any Critical Assets. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE1: 1) incorporated the best practice of making an electronic copy of all CIP related submittals and documents and will save the compliance-related records within an electronic document retention program; 2) entered relevant CIP-002 activities into a corporate managed monitoring database, which will automatically send annual reminders to the CIP senior manager or delegate(s) to review, update as necessary, and approve SERC_URE1's RBAM, list of Critical Assets, and list of Critical Cyber Assets; and 3) hired a full time environmental and regulatory compliance manager, responsible for the development, planning, implementation, and maintenance of an effective facility compliance program. SERC has verified the completion of all mitigation activity.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013011923	CIP-002-3	R4	During a scheduled Compliance Audit, the SERC audit team reported that SERC_URE1 had an issue with CIP-002-3 R4 because it failed to annually approve the risk based assessment methodology (RBAM), list of Critical Assets and list of Critical Cyber Assets (CCAs) for one year. After further assessment, SERC determined that SERC_URE1 did not annually approve its RBAM, Critical Asset list, and CCA list for two years.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1 had applied its RBAM annually before and after the missed year and did not identify any Critical Assets. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE1: 1) incorporated the best practice of making an electronic copy of all CIP related submittals and documents and will save the compliance-related records within an electronic document retention program; 2) entered relevant CIP-002 activities into a corporate managed monitoring database, which will automatically send annual reminders to the CIP senior manager or delegate(s) to review, update as necessary, and approve SERC_URE1's RBAM, list of Critical Assets, and list of Critical Cyber Assets; and 3) hired a full time environmental and regulatory compliance manager, responsible for the development, planning, implementation, and maintenance of an effective facility compliance program. SERC has verified the completion of all mitigation activity.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC2013011924	CIP-003-1	R2	During a scheduled Compliance Audit, the SERC audit team reported that SERC_URE1 had an issue with CIP-003-3 R2 because it failed to identify the CIP senior manager by name, title and date of designation prior to the enforceable period. SERC_URE1 failed to properly assign a senior manager as of the date the Standard became mandatory and enforceable for SERC_URE1. Instead, SERC_URE1's parent company delegated power to and authorized SERC_URE1's manager to sign any documentation required to establish compliance with NERC Reliability Standards. This delegation failed to identify the manager by name and only included the title of the manager and date of delegation. SERC also determined that SERC_URE1 changed the individual authorized to sign documentation required to establish compliance with NERC Reliability Standards but failed to document that change within 30 calendar days, and instead took 43 days to document the change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SERC_URE1's parent company authorized the manager to sign any documentation required to establish compliance with NERC Reliability Standards. SERC_URE1 was 13 days late in documenting the change to the individual authorized to sign documentation required to established compliance with NERC Reliability Standards. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4.	To mitigate this issue, SERC_URE1: 1) produced a document that properly designates a single CIP senior manager; 2) created a key managerial transition checklist to review in the event that a key manager, including the CIP senior manager, leaves the company, in order to delegate such a manager's duties to other employees as necessary until a suitable replacement can be found; and 3) entered relevant CIP-003 activities into a corporate managed monitoring database, which will automatically send an annual reminder to the CIP senior manager and any delegate(s) to assign a CIP senior manager and identify that individual pursuant to CIP-003, document changes to the CIP senior manager within 30 calendar days, document any delegations of authority, and authorize and document any exceptions to SERC_URE1's cybersecurity policy. SERC has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NRCXXXXX	SPP2013012175	CIP-003-1	R4	During a CIP Compliance Audit of SPP_URE1, the Audit Team found that SPP_URE1 had an issue with CIP-003-1 R4. SPP_URE1 had not classified as confidential its recovery plan for its physical access control system, its response plan, and its corporate procedure for all incident reporting and responding, as required by its information protection program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although SPP_URE1 had failed to mark the three documents in accordance with its information protection program, SPP_URE1 did closely control access to these documents. The electronic versions of these confidential documents were username and password protected, secured within SPP_URE1's Electronic Security Perimeter, and available to only those with approved access. The hardcopies of these confidential documents were protected behind access-controlled doors.	To mitigate this issue, SPP_URE1 marked its physical access control system recovery plan, response plan, and corporate procedure for all incident reporting and responding as confidential. As a preventative measure, SPP_URE1 changed its procedures to ensure electronic file names are classified "confidential" if the actual document cannot be marked. SPP RE has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NRCXXXXX	SPP2013012183	CIP-007-3	R5.3; R5.3.1; R5.3.2; and R5.3.3	During a CIP Compliance Audit of SPP_URE1, the Audit Team found that URE1 had an issue with CIP-007-3 R5.3. SPP_URE1's administrator account for its storage area network (SAN) could not technically enforce the password complexities required in R5.3.1, R5.3.2, and R5.3.3. SPP_URE1 did not request a Technical Feasibility Exception (TFE) for the subject account. Additionally, through the course of mitigating this issue, SPP_URE1 noted that three other devices, two network switches within its primary energy management system (EMS) and one network switch within its backup EMS, could not technically enforce the password complexities required in R5.3.1, R5.3.2, and R5.3.3. Similarly, SPP_URE1 had not requested a TFE for these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. URE1's SAN administrator account and network switches were accessible only locally, no remote access possible, and used by authorized staff to manage the device. Furthermore, these devices did have password protection despite the fact that they did not have the ability to enforce the required password complexities. Finally, the SAN device and the network switches were protected within a CIP Physical Security Perimeter.	To mitigate this issue, SPP_URE1 filed two TFEs to exclude the SAN devices and network switches from enforcing the password complexity requirements. SPP_URE1's TFE's compensating measures, which have already been implemented, include randomly generating passwords through a program capable of enforcing the password complexities of CIP-007-3 R5.3.1 and R5.3.2, and manually inputting those generated passwords into the excluded devices, and manually changing passwords on affected devices at least annually. SPP RE has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NRCXXXXX	SPP2013012179	CIP-006-1	R3	During a CIP Audit of SPP_URE1, the Audit Team found that URE1 had an issue with CIP-006-1 R3 because SPP_URE1 did not have documented its technical and procedural controls that were implemented for monitoring of physical access at all access points to its Physical Security Perimeters (PSPs).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although URE1 did not document its technical and procedural controls for monitoring physical access to all access points to its PSP, the SPP RE Audit Team determined that SPP_URE1 sufficiently monitored physical access to its PSPs. SPP_URE1's PSPs were afforded the protective measures of CIP-006-1 R3. SPP_URE1 had alarm contacts on its doors to alert on forced and held door-related events; alarms on its door controller panel boxes to alert anytime the panel door was opened; and a physical access control system alarm to alert on unauthorized badge access attempts. This issue was documentation-related.	SPP_URE1 revised its physical security program to include its implemented procedural controls for monitoring physical access at all access points to its PSPs. SPP RE verified that all mitigating activities were completed.

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NRCXXXXX	SPP2012010239	CIP-003-3	R4	During a CIP Compliance Audit of SPP_URE2, SPP RE found that SPP_URE2 had an issue with CIP-003-3 R4. SPP_URE2 did not protect Critical Cyber Asset (CCA) information in accordance with its documented CIP information protection program (Program). Specifically, SPP_URE2's Program requires CCA information to be encrypted if transmitted externally. SPP_URE2 transmitted externally 10 hard drives which contained unencrypted CCA information. Because SPP_URE2 did not encrypt the CCA information on the hard drives prior to transmitting it externally, SPP_URE2 did not protect its CCA information in accordance with its Program and CIP-003-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SPP_URE2 attested that the host files from all 10 hard drives were deleted prior to transmitting them for destruction. By deleting the host files, had the 10 hard drives been intercepted by a third party, no CIP protected information would have been accessible without the use of special software to recover the information. This was the only occurrence SPP_URE2 used a carrier to transfer hard drives from one facility to another.	To mitigate this issue, SPP_URE2: 1) updated its Program by clarifying language addressing the encryption of CCA information transmitted externally; and 2) acquired degaussers, a process that erases data, to aid in destroying electronic CIP information on hard drives, at its facility. SPP RE has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP_URE3)	NRCXXXXX	SPP2012011100	CIP-005-3	R4; R4.2; R4.3	During a Compliance Audit of SPP_URE3, SPP RE determined that SPP_URE3 had an issue with CIP-005-1 R4. SPP_URE3's cyber vulnerability assessment (CVA) was insufficient to ensure the discovery of all access points to the Electronic Security Perimeter (ESP), as required by CIP-005-1 R4.3. Also, the CVA was insufficient to ensure that the ports and services enabled on one asset, an internal network switch, were required for operations in accordance with CIP-005-1 R4.2. Regarding R4.3, the SPP_URE3 networks were scanned from within the ESP and externally from the Internet to discover all access points. However, the CVA team did not perform a secondary physical inspection of network wiring to identify any access points not identified in the network scans. Additionally, SPP_URE3 did not designate one internal network switch as an electronic access point. Regarding R4.2, SPP_URE3 did not verify that the network switch's enabled ports and services were required for operations.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SPP_URE3's CVA involved a review of the SPP_URE3 network topology and included network mapping/vulnerability scanning, which identified all externally communicating network access points (gateways), but SPP_URE3 failed to identify one internal network switch access point. The internal network switch resided on an isolated network segment and only served as a connection point for one remote workstation that communicated with the ESP via a virtual private network (VPN) tunnel. A user at the remote workstation is required to supply a physical token, username, and password before a VPN session can be established, and the session can only be established via the remote workstation. The enabled ports and services on the remote workstation were reviewed as part of the CVA and were subsequently determined to be necessary for operations. The port and service hardening of the remote workstation in combination with the requirement to establish a VPN session between the workstation and ESP firewall negated the risk presented by the lack of a review of ports and services on the network switch. Moreover, any communications passing from the remote workstation through the ESP firewall would have been inspected by the SPP_URE3 ESP firewall anti-virus and the ESP intrusion prevention system.	To mitigate this issue, SPP_URE3: 1) conducted a CVA that included a physical inspection of all network equipment and devices within the ESP to ensure the discovery of all access points to the ESP; and 2) decommissioned the isolated workstation that was communicating remotely via the implicated switch, thereby eliminating the switch as an access point. SPP RE has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP_URE4)	NRCXXXXX	SPP2012010962	CIP-007-1	R6; R6.1	During a CIP Compliance Audit of SPP_URE4, the Audit Team found that SPP_URE4 had an issue with CIP-007-1 R6. SPP_URE4 had not implemented automated tools or organizational process controls to monitor system events that relate to cyber security for all Cyber Assets within its Electronic Security Perimeter (ESP). Specifically, 21.4% of supervisory control and data acquisition (SCADA) network switches, which monitor system events related to cyber security, were not configured to send automated log messages to a SPP_URE4's server. The syslog server is configured to send alerts to operating personnel for emergent security events across SPP_URE4's ESP. Two of the three switches are located in SPP_URE4's back-up control center and one switch is located in SPP_URE4's primary control center.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The three switches involved, which are not Critical Cyber Assets and which are housed within a physical security perimeter, connect a SPP_URE4 control center and back-up control center to switches at SPP_URE4's primary and back-up control centers (Control Center Switches). The Control Center Switches were properly configured for logging security events in accordance with CIP-007 R6. Therefore, the syslog server still would have alerted operating personnel of any cyber security incidents that occurred on traffic between the three switches and the Control Center Switches. Furthermore, SPP_URE4's primary control center had one switch, Switch A, which was properly configured to send logs to the syslog server. Finally, SPP_URE4 had an intrusion detection system that monitors the ESP network for malicious activities and produces reports to personnel in a security management station.	To mitigate this issue, SPP_URE4: 1) modified the configurations of the three SCADA network switches so that they will be monitored and have the capability to send automated log messages to the syslog server; and 2) modified its cyber vulnerability assessment procedures to include a review of Cyber Assets to ensure that log messages from the three switches are sent to syslog servers.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP_URE4)	NRCXXXXX	SPP2012010878	CIP-006-3c	R1; R1.6.2	SPP_URE4 submitted a Self-Report stating that it had an issue with CIP-006-3c R1.6.2 for failing to provide continuous escorted access for two visitors within its Physical Security Perimeter (PSP). The two visitors, which were maintenance personnel, entered a secured conference room within a SPP_URE4 control center PSP without an escort as an SPP_URE4 employee was leaving the conference room. The visitors remained in the secured area for nine minutes while changing the filters on the heating, ventilation, and air conditioning system, and then exited the conference room.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the conference room is within SPP_URE4's control center PSP, the room does not have any Critical Cyber Assets (CCAs) and is separated by controlled access, e.g., magnetically locked doors with card key access and automated alarms, from the control center. Had the visitors attempted to access the control center, an alarm would have been sent to SPP_URE4 security personnel to investigate. Additionally, SPP_URE4's control center is manned by operators twenty-four hours a day, seven days a week. Had the visitors gained access to the control center, control center operators would have observed the unauthorized visitors and immediately escorted them out of the secured area. SPP_URE4 confirmed that the visitors did not attempt to enter the control center.	SPP_URE4 verbally counseled the visitors to ensure their understanding of SPP_URE4's escorting procedures. Additionally, SPP_URE4 retrained all affected personnel with authorized physical access to CCAs on the escorting procedures. SPP RE verified that all mitigating activities were completed.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 5 (SPP_URE5)	NRCXXXXX	SPP2013011796	CIP-003-1	R6	SPP_URE5 submitted a Self-Report stating that it had an issue with CIP-003-1 R6. SPP_URE5 did not follow its documented change control and configuration management process for adding, modifying, replacing, or removing Critical Cyber Asset (CCA) hardware or software. Specifically, SPP_URE5's change control and configuration management process designated a SPP_URE5 director as the approver for changes to CCAs. However in the tracking system for such changes a SPP_URE5 senior engineer approved changes made to its CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although SPP_URE5's senior engineer was not designated to approve changes per SPP_URE5's documented process for change control and configuration management, it was determined that the changes to CCAs approved by the senior engineer would have been approved in the same manner by SPP_URE5's director.	To mitigate this issue, SPP_URE5 changed the designated approver in the tracking system to the designated approver in SPP_URE5's documented process for change control and configuration management to ensure that the director was approving all changes to its CCAs. SPP RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NRCXXXXX	TRE2012009903	CIP-002-1	R1.2.1	Texas RE conducted an Audit of TRE_URE1 and determined that TRE_URE1 had an issue with Reliability Standard CIP-002-1 R1.2.1. TRE_URE1 did not consider and evaluate control centers and backup control centers performing the functions of the entities listed in the Applicability section of this Standard under its risk-based assessment methodology (RBAM). As of the applicability date for CIP-002-1, TRE_URE1's RBAM did not include consideration for a third-party control center that was performing some of TRE_URE1's day-ahead schedules and real-time communications. The issue period lasted for about two years and two months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. Although TRE_URE1 failed to include a third-party control center in its RBAM, this control center was not considered a Critical Asset. During the issue period, TRE_URE1 had not identified any Critical Assets or Critical Cyber Assets (CCAs) through the application of its RBAM for the remainder of its system. After TRE_URE1 did include this control center in its RBAM, TRE_URE1 re-performed the application of its RBAM, and still did not identify any Critical Assets or CCAs, confirming that this control center was not critical or in need of Critical Asset or CCA status throughout the issue period. The third-party control center is used as a communications medium between the generation unit and other entities and does not perform any of the operations related to the generation unit.	To mitigate this issue, TRE_URE1: 1) submitted its updated RBAM to Texas RE, which included a consideration of TRE_URE1's third-party control center; 2) re-performed its RBAM and did not identify any Critical Assets or CCAs at this generation station or any of its assets; 3) developed a new procedure intended to ensure that all assets are considered and evaluated when performing its RBAM. This measure was developed in order to directly reduce the risk of recurrence of this violation. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE2012010027	CIP-002-1	R2	Texas RE performed an Audit of TRE_URE2 and determined that TRE_URE2 failed to correctly apply its risk-based assessment methodology (RBAM) in accordance with Reliability Standard CIP-002-1 R2. First, when applying its RBAM, TRE_URE2 failed to consider the control centers and backup control centers of its contractor. Second, TRE_URE2's original Critical Asset list incorrectly identified the plant control room as a Critical Asset. The control room should not have been placed on the list for about two years.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. TRE_URE2 later considered the control centers and backup control centers of its contractor and TRE_URE2 determined that it had no additional CAs. TRE_URE2 had properly identified the other CAs on its CA list at the time of the issue. The third-party control center contractor is used as a communications medium between the generation unit and other entities and does not perform any of the operations related to the generation unit. Additionally, TRE_URE2 has only one generating asset that contributes a small amount of generation to the system.	To mitigate this issue, TRE_URE2: 1) correctly considered the third-party contractor the control centers and backup control centers; and 2) correctly applied its RBAM; Texas RE has verified the completion of all mitigation activity.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE2012010030	CIP-002-1	R3	Texas RE conducted an Audit of TRE_URE2, and determined that TRE_URE2 did not properly identify its Critical Cyber Assets (CCA) in accordance with Reliability Standard CIP-002-1 R3. For about two years, TRE_URE2 included in its list of CCAs several assets that were critical to the operation of two TRE_URE2 Critical Assets. However, these assets did not use a routable protocol to communicate outside the Electronic Security Perimeter, did not use a routable protocol within a control center, or were not dial-up accessible. Therefore, those assets did not meet the requirements of a CCA to be identified under CIP-002-1 R3, and should not have been included in TRE_URE2's list of CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because TRE_URE2 did not have any CCAs once TRE_URE2 correctly developed its list. TRE_URE2 had properly identified the other CAs on its CA list at the time of the issue. The third-party control center contractor is used as a communications medium between the generation unit and other entities and does not perform any of the operations related to the generation unit. Additionally, TRE_URE2 is only one generating asset that contributes a small amount of generation to the system.	To mitigate this issue, TRE_URE2 correctly identified that it had no CCAs. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE2012009737	CIP-005-3a	R5.3	On TRE_URE3 submitted a Self-Report to Texas RE, stating that it had an issue with CIP-005-3a R5.3. TRE_URE3 did not retain electronic access logs for 90 calendar days. TRE_URE3's Energy Management System (EMS) administrator discovered that the logging for one firewall in the Electronic Security Perimeter (ESP) for the new control center was incorrectly configured when installed. This resulted in no logs being retained for that device for about one month.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because all systems are behind a firewall that only allows the ports and services that are required for the system to function. All systems inside the ESP were logged for access during the time period of this issue. TRE_URE3 has stated that there were no incidents of unauthorized access attempts.	To mitigate this issue, TRE_URE3 EMS staff corrected the firewall configuration to send logs and installed a new application server at the backup control center, which will significantly reduce the likelihood of logs being lost in the future. Logs for the firewall are now being retained as required. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE2012011385	CIP-006-3c	R7	TRE_URE3 submitted a Self-Report to Texas RE stating that it had an issue with CIP-006-3c R7. TRE_URE3 discovered that the Physical Security Perimeter (PSP) access logs for approximately eight hours for one day were missing. Therefore, the TRE_URE3 failed to retain physical access logs for at least 90 calendar days as required by CIP-006-3c R7.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because TRE_URE3 identified no evidence of a cyber attack or physical intrusion related to the missing logs. Furthermore, access badges continued to work as expected during the pendency of the issue, protecting the security of TRE_URE3 Critical Cyber Assets.	To mitigate this issue, TRE_URE3 installed new software, including an upgraded version of the archival database for the logging system. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4)	NCRXXXXX	TRE2012010554	CIP-005-1	R1	During a Compliance Audit of TRE_URE4, Texas RE determined that TRE_URE4 had an issue with CIP-005-1 R. TRE_URE4 misidentified access points to the Electronic Security Perimeter (ESP). For these access points, TRE_URE4 erroneously identified systems having external programmatic access to the ESP which were termed "highlighted cloud bubbles" or "clouds." The clouds did not go to the perimeter of the ESP. They went to the firewall. Therefore, TRE_URE4 did not identify access points to the perimeter of the ESP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because although TRE_URE4's documentation misidentified the access point in one case and did not label the access point in another, TRE_URE4 understood and treated the firewall controlling electronic access to the ESP as the de facto access point. TRE_URE4 treated the de facto access point as the access point, but did not document it as the access point pursuant to CIP-005 R1.	To mitigate this issue, TRE_URE4: 1) revised its process document to appropriately identify the access point; and 2) updated its network diagram, adding an access point label. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 5 (TRE_URE5) CPS Energy - DP-LSE-TO-TOP-TP (CPS)	NCRXXXXX	TRE201100558	CIP-006-1	R1	After an Audit, Texas RE determined that TRE_URE5 created a physical security plan but failed to show approval by the designated senior manager or delegate(s) for its physical security plan Version 2. A review of the evidence shows that neither the senior manager nor the delegate signed the physical plan, representing a failure to approve the plan by the designated CIP senior manager or delegate. Specifically, the plan was reviewed and signed by a TRE_URE5's officer and the delegate's direct manager, even though neither was the assigned delegate. The issue was resolved when the next year's physical security plan Version 3 was reviewed and approved by the designated authority in the fall. TRE_URE5 had an issue with CIP-006-1 R1 for about one year and eight months.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). TRE_URE5's physical security plan has been reviewed by the delegated personnel on an annual basis and has been in effect since the Standard became enforceable. The absence of the expected signature was attributed to a misinterpretation of the signature block title, not an indication that the plan was not approved or reviewed. Texas RE determined that the instant issue is appropriate for FFT treatment because TRE_URE5 identified and mitigated the issue before the Audit commenced.	To mitigate this issue, TRE_URE5 provided documentation showing that the delegated signatory signed Version 3 of the physical security plan. Texas RE verified completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 6 (TRE_URE6)	NCRXXXXX	TRE2012010294	CIP-005-1	R4.2, R4.3, R4.4	During an Audit, TRE_URE6 reported that its diagnostic cyber vulnerability assessment (CVA) data was not accessible because the file containing the data was corrupted and not recoverable. Therefore, TRE_URE6, had an issue with CIP-005-1 R4. In response to this information loss, TRE_URE6 provided internal correspondence showing requests for data to validate that the CVA was conducted, responses to those requests, and work orders used to track time associated with acquiring the appropriate data. TRE_URE6 was able to construct a logical picture from internal correspondence showing that its CVA process and resulting documented assessment was systematically acquired and disseminated to the appropriate parties, which enabled TRE_URE6 to reach the conclusions presented in its CVA assessment. The associated process documents defining TRE_URE6's approach to conducting CVAs were in accordance with CIP-005-1 R4.1, and the results produced from the CVA were also in accordance with CIP-005-1 R4.5. However, TRE_URE6 failed to provide evidence that a review of ports and services required for operations, discovery of all access points to the Electronic Security Perimeter (ESP), and a review of controls for default accounts, passwords, and network management community strings was performed. Therefore, Texas RE determined that TRE_URE6 had an issue with CIP-005-1 R4.2, R4.3, and R4.4 for about one year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TRE_URE6 performed its CVA, implemented a layered approach to protecting its Cyber Assets that included firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and ESP and Physical Security Perimeter (PSP) access authentication. In addition, TRE_URE6 improved security by adding third-party assessments to facilitate hardening of its protection scheme. TRE_URE6 also provided evidence that missing data from the corrupted CVA assessment was requested and delivered to the appropriate TRE_URE6 parties. A review of evidence shows that TRE_URE6 followed procedures and performed a review resulting in changes to its network to close ports discovered open on oen of its servers. TRE_URE6 supplied the work order generated to correct the network deficiencies discovered from the CVA. This layered protection was partially based on the information collected in response to the lost CVA diagnostic data.	To mitigate this issue, TRE_URE6 hired a third-party vendor to perform CVAs and retain the results for historical access. All future TRE_URE6 CVAs will be performed by this method. Texas RE verified completion of all mitigation activity.

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 6 (TRE_URE6)	NCRXXXXX	TRE2012010296	CIP-007-1	R8.2, R8.3	During an Audit that concluded on May 11, 2012, TRE_URE6 reported that its diagnostic cyber vulnerability assessment (CVA) data was not accessible because the file containing the data was corrupted and not recoverable. Therefore, TRE_URE6, had an issue with CIP-007-1 R8. In response to this information loss, TRE_URE6 provided internal correspondence showing requests for data to validate that the CVA was conducted, responses to those requests, and work orders used to track time associated with acquiring the appropriate data. TRE_URE6 was able to construct a logical picture from internal correspondence that its CVA process and resulting documented assessment was systematically acquired and disseminated to the appropriate parties, which enabled TRE_URE6 to reach the conclusions presented in its CVA assessment. The associated process documents defining TRE_URE6's approach to conducting CVAs were in accordance with CIP-007-1 R8.1, and the results produced from the CVA were also in accordance with CIP-007-1 R8.4. However, TRE_URE6 failed to provide evidence that a review of ports and services required for operations of Cyber Assets and a review of controls for default accounts was performed. Therefore, Texas RE determined that TRE_URE6 had an issue with CIP-007-1 R8.2 and R8.3 for a period of one year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TRE_URE6 implemented a layered approach to protecting its Cyber Assets that includes firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and Electronic Security Perimeter (ESP) and Physical Security Perimeter (PSP) access authentication. In addition, TRE_URE6 has improved security by adding third-party assessments to facilitate hardening of its protection scheme. TRE_URE6 also provided evidence that missing data from the corrupted CVA assessment was requested and delivered to the appropriate TRE_URE6 parties. A review of evidence shows that TRE_URE6 followed procedures and performed a review of the CVA. As a result, TRE_URE6 implemented changes to harden its network through tightening access privileges and ensuring identified vulnerabilities were patched. TRE_URE6 supplied the work order generated to correct the network deficiencies discovered during the CVA.	To mitigate this issue, TRE_URE6 hired a third-party vendor to perform CVAs and retain the results for historical access. All future TRE_URE6 CVAs will be performed by this method. Texas RE verified completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 7 (TRE_URE7)	NCRXXXXX	TRE201100481	CIP-007-1	R6; R6.4; R6.5	TRE_URE7 submitted a Self-Report stating that it did not retain logs for 43 of its Cyber Assets within the Electronic Security Perimeter (ESP) for 90 calendar days as required by CIP-007-1 R6.4. Upon further review, TRE_URE7 also determined that required logs on domain controllers were not retained. Additionally, TRE_URE7 discovered that some of its devices were collecting logs but that those logs failed to contain all events as required by TRE_URE7's company procedure. TRE_URE7's investigation showed that the failure to retain logs was caused by (1) a failure of an application process to transmit the logs of system events to the designated repository; (2) lack of accessibility to system event logs for certain devices; and (3) limited storage space available in each affected Cyber Asset to maintain the required logs. In addition, as part of that same self-assessment, TRE_URE7 discovered that for 50 of its devices, it failed to review certain logs of system events and to maintain documentation of all reviews related to cybersecurity as required by CIP-007-1 R6.5. The failure to conduct the review of the logs was caused by a failure to appropriately execute the review process. Therefore, TRE_URE7 had an issue with CIP-007-1 R6 for about two years and a half.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although logging and documentation of log reviews were not maintained, alerts were being generated by the firewalls and intrusion detection system equipment, and those alerts were investigated. Those alerts were automated and performed in real-time. The results of those investigations were documented. At no time during the pendency of this issue, did TRE_URE7 experience a system event that presented a risk to the BPS. TRE_URE7's real-time alerting from firewalls and intrusion detection systems supports TRE_URE7's ability to detect security related events and take corrective action before a 90-day log review is required by the Standard.	TRE_URE7's investigation found the root cause to be that employees did not have a clear understanding of their responsibilities and accountability for the review of event logs. TRE_URE7 has taken several steps to prevent or minimize the probability of incurring further issues of the same or similar Standard, including adding a director of internal audit to the functional organization responsible for this area, and reorganizing the group responsible for implementation of CIP-007 to provide added focus to the tactical responsibilities of CIP implementation, enhancing the log review procedure to provide clear responsibilities and accountability for event log review, and taking appropriate actions with employees through the performance review process. To mitigate this issue, TRE_URE7: 1) verified log collection for all Cyber Assets within the EPS; 2) performed reviews required by TRE_URE7's log review procedures; 3) established Mitigation Plan team; 4) reviewed TRE_URE7's existing applicable procedures; 5) investigated logging capabilities of storage area network devices; 6) conducted compliance procedure refresher training; 7) installed log transmittal alerting that monitors the connection between log collectors and their associated repositories; and 8) implemented new network equipment log collector process. Texas RE verified completion of all mitigation activity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 8 (TRE_URE8)	NCRXXXXX	TRE201100548	CIP-007-2a	R3	TRE_URE10 self-certified that it had procedures and personal performance goals in place for conducting a 30-day assessments of security patches, which requires responsible employees to capture evidence. However, the employees responsible did not capture evidence for all of the assessments. Therefore, TRE_URE8 did not have sufficient documented evidence to show all assessments of security patches were performed within 30 days of availability from the vendor(s). This issue lasted about four months and a half.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because TRE_URE8 had several layers of mitigating and compensating measures. First, TRE_URE8 performed but did not document the assessments at issue. Second, the systems at issue are non-critical Cyber Assets that do not reside within the same Electronic Security Perimeter as Cyber Assets performing real-time control center functions. Third, several layers of compensating measures were in place including: a) electronic access was controlled via five means, including authentication services; b) physical access was protected via biometric controls; c) automated electronic processes for log monitoring and collection were in place where technically feasible – no issues were noted; d) electronic intrusion detection systems were in place; e) the operating systems were securely configured to protect against unauthorized access; and f) antivirus and antimalware software was installed.	TRE_URE8 assessed and documented evidence to show all assessments of security patches were performed within 30 days of availability. Texas RE has verified the mitigation activities as complete.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2013011962	CIP-005-3	R1; R1.5	WECC issued WECC_URE1 a Notice of Compliance Audit indicating WECC would conduct an onsite Compliance Audit. The WECC Audit Team conducted onsite interviews with WECC_URE1 Subject Matter Experts (SMEs). During the course of one interview WECC_URE1 disclosed that it had failed to ensure one Cyber Asset used in the access control and/or monitoring (ACM) was afforded the protections described in CIP-007-3 R6.2, as required under CIP-005-3 R1.5. Specifically, WECC_URE1 reported that it failed to ensure the device was configured to issue automated or manual alerts for detected cybersecurity incidents. The device was logging events, but the events were not configured to alert appropriate personnel.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The scope of the violation is limited to a single ACM device. The ACM device is a console works log management server used to monitor and log access to an ESP. Although the device did, in fact, log and monitor access, it was not configured to issue automated alerts signaling a cybersecurity incident. WECC_URE1 electronically secured the ESP with other protections in place during the duration of the issue. WECC_URE1 provided 17 out of 18 protections required under R1.5 to the device. WECC_URE1 restricted electronic and physical access to the device. WECC_URE1 located the device within a Physical Security Perimeter (PSP). Individuals with access to the device had completed personnel risk assessments. Individuals with access were listed pursuant to CIP-004-3 R4. WECC_URE1 staff reviewed the access lists on a quarterly basis. WECC_URE1 logged and monitored all electronic access through the device. Unauthorized electronic access attempts would have been detected and triggered alarms. Only ports and services required for operations and for monitoring Cyber Assets within the ESP were enabled. The device was equipped with antivirus software and malicious software prevention tools. WECC_URE1 restricted electronic access to the ESP using passwords. Further, given "layered" security approach adopted by WECC_URE1, cybersecurity events within the ESP would have been detected and triggered alarming by other Cyber Assets within the ESP.	To mitigate this issue WECC_URE1 reconfigured the device to ensure that automated alerts were issued in the event of a cybersecurity incident.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2013012037	CIP-004-3	R3; R3.2	WECC_URE2 submitted s Self-Certification to WECC stating that it had an issue with CIP-004-3 R3. Specifically, WECC_URE2 reported that it failed to update a personnel risk assessment (PRA) for a single employee after the initial PRA performed seven years earlier. The employee's PRA was updated approximately 18 months after it was due for completion.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The individual previously completed a PRA and is an employee in good standing. The individual was and is up-to-date with cybersecurity training. The individual in scope of the issue maintained physical access to Critical Cyber Assets (CCAs) associated with a single substation. Physical access to the CCAs was monitored on a 24 hours a day, seven days a week basis by security personnel using a live video feed. WECC_URE2 logged physical access was logged through a card reader and associated database.	To mitigate this issue, WECC_URE2: 1) revoked the employee's access to CCAs; 2) completed a PRA update for the employee before it reinstated the employee's access privileges to CCAs; 3) updated its business process to ensure that all PRAs are updated within seven years; and 4) trained all WECC_URE2 employees and contractors on the updated business process to ensure that PRAs are updated within seven years.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2012009678	CIP-007-3a	R6	WECC_URE3 submitted a Self-Report to WECC stating that it had an issue with CIP-007-3 R6. Specifically, WECC_URE3 reported that it failed to implement protective measures prescribed under R6 where technically feasible, for a single Cyber Asset. WECC determined that WECC_URE3 deployed a Cyber Asset that did not have automated tools or organizational process controls to monitor system events as technically feasible as required under R6. WECC also determined that because implementation of technical measures to facilities monitoring is technically infeasible on this device, this issue stems from WECC_URE3's failure to file a timely technical feasibility exception (TFE) request.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE3 had compensating protective measures in place during the duration of the issue. The scope of the issue is limited to a single Cyber Asset. Although WECC_URE3 failed to file a timely TFE, WECC_URE3 did ensure that the device was located within an Electronic Security Perimeter, pursuant to CIP-005, wherein system events are monitored and electronic access thereto is controlled. Further the device was physically secured within a Physical Security Perimeter and afforded protections that ensure the physical security of the device.	To mitigate this issue, WECC_URE3: 1) created a database audit function for TFEs that compares the device classification, make, and model to the CIP standards and information related to previously submitted TFEs. The audit function will flag devices that should have a TFE, but have not been accounted for in previous TFE amendments; and 2) amended its previous TFE to include the device. WECC approved the TFE.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010115	CIP-006-1	R1; R1.8	WECC_URE4 submitted a Self-Report to WECC stating that it had an issue with CIP-006-1 R1. WECC conducted a Compliance Audit of WECC_URE4's compliance with, among other Reliability Standards, CIP-006-1 R1. The Audit Team reviewed WECC_URE4's Self-Report during its Compliance Audit. According to the Audit Team, WECC_URE4 failed to afford its Cyber Assets the protective measures in Reliability Standards CIP-007-1 R5.2.3, as well as CIP-007-1 R5.3 as required by CIP-006-1 R1.8. With respect to CIP-007-1 R5.2.3, WECC_URE4 failed to change shared accounts on its access control software when personnel changes occurred. With respect to CIP-007-1 R5.3, WECC_URE4 failed to implement technical and procedural controls by having passwords to its Physical Access Control Systems (PACS) that were sufficient in complexity, length, and frequency of password changes.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Logical access to the workstations involved and physical access to the Physical Security Perimeter was revoked when personnel changes occurred. In addition, all of WECC_URE4's passwords are managed by its active directory server, which enforces password complexity rules and expirations.	To mitigate this issue, WECC_URE4 disabled the shared account, implemented individual user accounts, and implemented technical and procedural controls of account and password management. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010267	CIP-007-3a	R5	WECC performed ~~an~~ Compliance Audit of WECC_URE4's compliance with, among other Reliability Standards, CIP-007-3 R5. According to the Audit Team, WECC_URE4 failed to provide evidence that it changed its passwords for its admin/shared/services accounts for one calendar year.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. As compensating measures, the accounts are not accessible outside a Physical Security Perimeter or an Electronic Security Perimeter. Thus, WECC_URE4 monitors and logs access to these accounts and only authorized WECC_URE4 personnel can gain access to the accounts. In action, the accounts are afforded the physical and electronic protections specified in CIP-005 and CIP-006.	To mitigate this issue, WECC_URE4 later produced evidence that it had changed its passwords for the previous calendar year and developed a new process for ensuring that all passwords are changed annually. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011869	CIP-007-1	R2; R2.3	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R2. Specifically, WECC_URE5 reported that it identified Cyber Assets that could not meet compliance with CIP-007-1 R2.3, but that did not have an associated technical feasibility exception (TFE). WECC_URE5 reported that although it was technically infeasible to disable unused ports or services for these devices, it failed to file a TFE.	There were a number of compensating measures in place to secure the devices against misuse or malicious attack. WECC_URE5 uses a security information and event management (SIEM) appliance to monitor system events and device event logs associated with the Cyber Assets in scope. The SIEM provides automated alerting of potential cybersecurity events associated with these devices as they occur by utilizing a display showing security events in real time. Cyber Assets are monitored 24 hours a day, seven days a week by SIEM. Further, WECC_URE5 utilizes malicious software prevention tools on all Cyber Assets associated with these devices within the Electronic Security Perimeter and Physical Access Control systems where technically feasible. In addition, WECC_URE5 submitted TFEs associated with these Cyber Assets. Although the TFEs were filed late, WECC approved all TFEs.	To mitigate this issue, WECC_URE5 filed TFEs for the devices. WECC approved the TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011870	CIP-007-1	R3; R3.2	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R3.2. Specifically, WECC_URE5 reported that it identified Cyber Assets that could not meet compliance with CIP-007-1 R3.2, but that did not have an associated technical feasibility exception (TFE). WECC_URE5 reported that although it was technically infeasible to install security patches for these devices, it failed to file a TFE.	There were a number of compensating measures in place to secure the devices against misuse or malicious attack. WECC_URE5 uses a security information and event management (SIEM) appliance to monitor system events and device event logs associated with the Cyber Assets in scope. The SIEM provides automated alerting of potential cybersecurity events associated with these devices as they occur by utilizing a display showing security events in real time. Cyber Assets are monitored 24 hours a day, seven days a week by SIEM. Further, WECC_URE5 utilizes malicious software prevention tools on all Cyber Assets associated with these devices within the Electronic Security Perimeter and Physical Access Control systems where technically feasible. In addition, WECC_URE5 submitted TFEs associated with these Cyber Assets. Although the TFEs were filed late, WECC approved all TFEs.	To mitigate this issue, WECC_URE5 filed TFEs for the devices. WECC approved the TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011871	CIP-007-1	R4	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R2. Specifically, WECC_URE5 reported that it identified Cyber Assets that could not meet compliance with CIP-007-1 R4, but that did not have an associated technical feasibility exception (TFE). WECC_URE5 reported that although it was technically infeasible to implement antivirus and anti malware solutions on the devices, it failed to file a TFE.	There were a number of compensating measures in place to secure the devices against misuse or malicious attack. WECC_URE5 uses a security information and event management (SIEM) appliance to monitor system events and device event logs associated with the Cyber Assets in scope. The SIEM provides automated alerting of potential cybersecurity events associated with these devices as they occur by utilizing a display showing security events in real time. Cyber Assets are monitored 24 hours a day, seven days a week by SIEM. Further, WECC_URE5 utilizes malicious software prevention tools on all Cyber Assets associated with these devices within the Electronic Security Perimeter and Physical Access Control systems where technically feasible. In addition, WECC_URE5 submitted TFEs associated with these Cyber Assets. Although the TFEs were filed late, WECC approved all TFEs.	To mitigate this issue, WECC_URE5 filed TFEs for the devices. WECC approved the TFEs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011873	CIP-007-1	R5; R5.3; R5.3.2; R5.3.3	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R5. Specifically, WECC_URE5 reported that it identified Cyber Assets that could not meet compliance with CIP-007-1 R5, but that did not have an associated technical feasibility exception (TFE). WECC_URE5 reported that although it was technically infeasible to enforce the use of strong passwords, it failed to file a TFE.	There were a number of compensating measures in place to secure the devices against misuse or malicious attack. WECC_URE5 uses a security information and event management (SIEM) appliance to monitor system events and device event logs associated with the Cyber Assets in scope. The SIEM provides automated alerting of potential cybersecurity events associated with these devices as they occur by utilizing a display showing security events in real time. Cyber Assets are monitored 24 hours a day, seven days a week by SIEM. Further, WECC_URE5 utilizes malicious software prevention tools on all Cyber Assets associated with these devices within the Electronic Security Perimeter and Physical Access Control systems where technically feasible. In addition, WECC_URE5 submitted TFEs associated with these Cyber Assets. Although the TFEs were filed late, WECC approved all TFEs.	To mitigate this issue, WECC_URE5 filed TFEs for the devices. WECC approved the TFEs.

Attachment A-2

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

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2013011874	CIP-007-1	R6	WECC_URE5 submitted a Self-Report to WECC stating that it had an issue with CIP-007-1 R6. Specifically, WECC_URE5 reported that it identified Cyber Assets that could not meet compliance with CIP-007-1 R6, and that did not have an associated Technical Feasibility Exception (TFE). WECC_URE5 reported that although it was technically infeasible to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity, it failed to file a TFE.	There were a number of compensating measures in place to secure the devices against misuse or malicious attack. WECC_URE5 uses a security information and event management (SIEM) appliance to monitor system events and device event logs associated with the Cyber Assets in scope. The SIEM provides automated alerting of potential cybersecurity events associated with these devices as they occur by utilizing a display showing security events in real time. Cyber Assets are monitored 24 hours a day, seven days a week by SIEM. Further, WECC_URE5 utilizes malicious software prevention tools on all Cyber Assets associated with these devices within the Electronic Security Perimeter and Physical Access Control systems where technically feasible. In addition, WECC_URE5 submitted TFEs associated with these Cyber Assets. Although the TFEs were filed late, WECC approved all TFEs.	To mitigate this issue, WECC_URE5 filed TFEs for the devices. WECC approved the TFEs.

Document Accession #: 20130530-5275 **Filed Date: 05/30/2013**

Document Content(s)