Federal Energy Regulatory Commission
Washington, D.C. 20426

Re:
Release Letter and Determination
Letter re: RC13-6
FOIA No. FY19-30

VIA EMAIL 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 December 16, 2021, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC13-6, along with the names of two (2) relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] Based on my own review of the relevant documents, I conclude that disclosure of these URE identities is appropriate and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC13-6

With respect to the remaining identities of UREs contained in RC13-6, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the

[1] 5 U.S.C. § 552 (2018).

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

Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC13-6 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: 2021.12.27 17:21:01 -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

RC13-6

February 28, 2013

Horse Hollow Generation Tie, LLC (HHGT)-.pdf page 24

Navajo Tribal Utility Authority (NTUA)-.pdf page 25

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 27 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 53 possible violations[5] of 15 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 53 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.

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

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.

[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).

Statement Describing the Resolution[8]

Basis for Determination

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

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

[8] *See* 18 C.F.R § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010).

Reliability Standard possible violations and confidential information regarding critical energy infrastructure.

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

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

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

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

cc: Entities listed in Attachment B

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 FEBRUARY 2013
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

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:

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

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

FOR WECC:

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

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

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

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

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
February 28, 2013

Take notice that on February 28, 2013, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding twenty-seven (27) Registered Entities in six (6) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Attachment A-1

February 28, 2013 Public Non-CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet (Non-CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Lake Road Generating Company, LP (Lake Road)	NCR07131	NPCC2011007724	VAR-002-1	R1	On July 22, 2011, Lake Road, as a Generator Operator, submitted a Self-Report to NPCC identifying an issue with VAR-002-1 R1. The Self-Report was submitted as a result of a NERC industry webinar that occurred on July 15, 2011 which clarified the notification obligation with respect to automatic voltage regulator (AVR) controls at generating facilities. Lake Road reported that since June 21, 2007, its three units had not been operating in automatic voltage control mode, but rather in reactive power control mode. Lake Road failed to notify the TOP that it was not operating in automatic voltage control mode, 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. Although the AVRs were controlling reactive power, Lake Road was following the voltage schedule provided by the Transmission Operator (TOP) at all times for the duration of the issue.	To mitigate this issue, Lake Road notified the TOP on July 22, 2011 that the plant was operating in the reactive power control mode. Lake Road tested the AVRs on the automatic voltage control mode, developed an operating procedure, and trained the generating control room operators on the correct control mode and notification to the TOP. NPCC has verified the completion of all mitigation activity.
Northeast Power Coordinating Council, Inc. (NPCC)	Lake Road Generating Company, LP (Lake Road)	NCR07131	NPCC2011007726	VAR-002-1	R3	On July 22, 2011, Lake Road, as a Generator Operator, submitted a Self-Report to NPCC identifying an issue with VAR-002-1 R3. The Self-Report was submitted as a result of a NERC industry webinar that occured on July 15, 2011 which clarified the notification obligations with respect to automatic voltage regulator (AVR) controls at generating facilities. Lake Road reported that since June 21, 2007, its three units had not been operating in automatic voltage control mode, but rather in reactive power control mode. Lake Road had misinterpreted the Standard and therefore had not notified its Transmission Operator (TOP) that the AVR was operating in the mode controlling reactive power and was outside the 30-minute notification requirement.	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 AVRs were controlling reactive power, Lake Road was following the voltage schedule provided by the Transmission Operator (TOP) at all times for the duration of the issue.	To mitigate this issue, Lake Road notified the TOP on July 22, 2011 that the plant was operating in the reactive power control mode. Lake Road tested the AVRs on the automatic voltage control mode, developed an operating procedure, and trained the generating control room operators on the correct control mode and notification to the TOP. NPCC has verified the completion of all mitigation activity.
Reliability*First* Corporation (Reliability*First*)	Chambers Cogeneration, LP (CCLP)	NCR00708	RFC2012011449	PRC-005-1	R1; R1.1	On November 13, 2012, CCLP, as a Generator Owner, self-reported an issue with PRC-005-1 R1.1. CCLP reported that its Protection System maintenance and testing program (Program) specified that instrument transformers are tested at plant commissioning and as required when problems are suspected. The Program did not include periodic maintenance and testing for these devices. During a self-assessment for compliance, CCLP determined that this method of maintenance and testing for instrument transformers does not appropriately address risk and may not be compliant with PRC-005-1.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. CCLP conducted testing on the instrument transformers at plant commissioning in October 1993. Based on recommendations from the devices' manufacturers, CCLP had not required periodic maintenance for instrument transformers. CCLP's Protection System uses many instrument transformers creating overlapping zones of protection, which ensures protection if a single instrument transformer should fail unexpectedly. Finally, upon performing maintenance and testing, CCLP determined the instrument transformers were operational and performed appropriately throughout the duration of the issue.	To mitigate the issue, CCLP: 1) scheduled testing of its instrument transformers; 2) completed all testing and reviewed the results; and 3) revised its Program to include a specific interval for testing instrument transformers.
Reliability*First* Corporation (Reliability*First*)	City of Cleveland, Dept. of Public Utilities, Division of Cleveland Public Power (CPP)	NCR00712	RFC2012001309	PRC-005-1a	R2	On January 11, 2012, CPP, as a Transmission Owner and Distribution Provider, self-reported an issue with PRC-005-1a R2.1. CPP self-reported that, in October 2011 and November 2011, it failed to timely complete monthly substation maintenance checks for 10 substations according to its Protection System maintenance and testing program (Program). At the West 41st Street, East Industrial, Pofok, and South East substations, October 2011 checks were conducted seven days late on November 7, 2011. At the Nottingham substation, November 2011 checks were conducted five days late on December 5, 2011. At the Division and Ridge Road substations, November 2011 checks were conducted six days late on December 6, 2011. At the Collinwood and Northeast substations, November 2011 checks were conducted eight days late on December 8, 2011. At the Lake Road substation, November 2011 monthly checks were conducted nine days late on December 9, 2011.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. CPP performed all maintenance checks within 10 days of the intervals set in the Program. Upon performing maintenance and testing, CPP determined all equipment was operable and would have performed appropriately if called upon during the duration of the issue.	To mitigate the issue, CPP: 1) revised its Program procedures to require maintenance activities to be completed earlier in the month, with an option for an approved extension, to ensure that tasks are complete by month's end even when unexpected circumstances place additional demand on operational personnel; 2) revised the Program procedures to include supervisor sign-off of completed and signed maintenance work forms and a process to request assistance for operational matters that avoids conflicts with scheduled reliability maintenance and testing; and 3) provided informal training to employees who perform the maintenance and testing to ensure they understand the procedure and policy changes.
Reliability*First* Corporation (Reliability*First*)	Duke Energy Corporation (Duke)	NCR00761	RFC2012011204	EOP-004-1	R3	On September 30, 2012, Duke, as a Balancing Authority, Generator Operator, Load Serving Entity, Transmission Operator self-reported an issue with EOP-004-1 R3 to Reliability*First*. On June 29, 2012, Duke experienced a customer outage that was a reportable incident pursuant to Attachment 2-EOP-004 because it affected more than 50,000 customers for at least one hour. Duke provided a copy of the preliminary written report to the U.S. Department of Energy (DOE), but Duke failed to provide a copy of the preliminary report to NERC and Reliability*First*. When it began to submit the final report, Duke discovered that due to a technological issue with the submittal software, it failed to submit the preliminary report to NERC and Reliability*First*. On July 2, 2012, Duke provided a copy of the final report to DOE, and provided a copy of both the preliminary report and final report to NERC and Reliability*First*.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). An issue with of EOP-004-1, R3 has the potential to affect the reliable operation of the BPS by enabling entities to incur reportable incidents of which DOE, NERC, and the Regional Entity are unaware. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. Duke timely submitted the preliminary report to DOE, and Duke submitted the final reports shortly after the reportable storm-related incident to DOE, NERC, and Reliability*First*.	To mitigate the issue, Duke reviewed and revised the current procedure for reporting disturbance events and reviewed procedure changes with employees responsible for reporting disturbances.
Reliability*First* Corporation (Reliability*First*)	PSEG Fossil LLC (PSEG Fossil)	NCR00893	RFC2012009966	PRC-005-1	R2	On March 21, 2012, PSEG Fossil, as a Generator Owner, self-reported an issue with PRC-005-1 R2 to Reliability*First*. PSEG Fossil relies on the local Transmission Owner, Public Service Electric & Gas Company (PSE&G) to perform maintenance and testing on its behalf for certain of its Protection System devices. During a discussion at the end of 2011 regarding the assignment of responsibility for future Protection System maintenance and testing, PSEG Fossil and PSE&G discovered that the last test record for the synchronizing breaker flash-over relay scheme associated with the Mercer Generating Station Unit No. 2 was from 2002. The flash-over relay scheme consists of two relays and a timer that operates in the event the breakers are open and there is either phase or ground current present. PSEG Fossil mistakenly believed that PSE&G was responsible for the maintenance and testing of this relay scheme. That relay had a maintenance and testing interval of five years, so PSEG Fossil failed to perform maintenance and testing on that relay scheme within the defined maintenance and testing interval. On December 27, 2011, PSEG Fossil performed maintenance and testing on the relays.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). A violation of PRC-005-1 R2 has the potential to affect the reliable operation of the BPS by allowing important Protection System devices to remain unmaintained and untested. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. PSEG Fossil has several relays that are part of the generator protection that can provide backup protection, including negative sequence relays and overcurrent relays. In addition, there are two fault detectors as part of the flashover scheme, and both must fail to lose all flashover protection. In addition, this issue affected only one relay scheme.	To mitigate the issue, PSEG Fossil: 1) performed outstanding maintenance and testing on the relays, reviewed all bulk electric system Protection System devices to ensure that all devices were within their maintenance and testing interval; 2) reviewed all Protection System devices that reside at the point of interconnection to ensure that no other Protection System devices lack clarity of ownership; and 3) completed an agreement between PSEG Fossil and PSE&G regarding maintenance and testing of relay schemes.
Reliability*First* Corporation (Reliability*First*)	PSEG Fossil LLC (PSEG Fossil)	NCR00893	RFC2012010420	VAR-002-1.1b	R3	On May 29, 2012, PSEG Fossil, as a Generator Operator self-reported an issue with VAR-002-1.1b R3 to Reliability*First*. On March 22, 2012, PSEG Fossil notified the Transmission Operator (TOP) that it would start a 628 MW generating unit's automatic voltage regulator (AVR) at the Bergen Generating Station in manual mode. When PSEG Fossil reset the AVR to automatic voltage control mode, however, PSEG Fossil failed to notify the TOP of this status change within 30 minutes. PSEG Fossil notified the TOP one hour after the status change, 30 minutes beyond the requisite notification period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Due to this failure to notify, the Balancing Authority remained unaware that the PSEG Fossil unit was ready for dispatch from minimum output levels, so for the 30 minute duration, the unit remained at minimum output level. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. PSEG Fossil has a defined procedure in place directing notification of the TOP that the operator failed to follow in this instance, demonstrating that this issue was an isolated occurrence. In addition, the operator notified the Transmission Owner, and PSEG Fossil notified the TOP 30 minutes after it was required to do so.	To mitigate the issue, PSEG Fossil: 1) reinforced the requirement of communicating all AVR changes to the generation desk with the station personnel involved in this incident; 2) disciplined the operator with a verbal reminder, which is the first level of discipline for the employee; and 3) gave the senior operations supervisor an adverse note in the leadership performance record.

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*)	Triton Power Michigan, LLC (Triton Power)	NCR11174	RFC2012010612	PRC-005-1a	R1	From April 30, 2012 to May 11, 2012, Reliability*First* conducted a Compliance Audit of Triton Power, as the Generator Owner for Jackson Power Company LLC. During the Compliance Audit, although Triton Power provided Reliability*First* with the Protection System maintenance and testing program (Program) revised on March 12, 2012, Reliability*First* did not review the Program. Triton Power had revised the Program after Reliability*First* sent a 90 day audit notification to Triton Power. During the Compliance Audit, Reliability*First* determined Triton Power did not include in its Program a basis or interval for its DC control circuitry and did not include a basis for its five-year interval for nickel cadmium batteries pursuant to PRC-005-1a R1.1. Additionally, Reliability*First* determined that Triton Power did not include in its Program a summary of maintenance and testing procedures for relays, voltage sensing devices, station batteries, and DC control circuitry pursuant to PRC-005-1a R1.2.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that the issue was a documentation error. During the Compliance Audit, Triton Power provided Reliability*First* with evidence demonstrating Triton Power performed maintenance and testing on its Protection System devices within defined intervals during the duration of the issue. Specifically, Triton Power was able to provide the last date of maintenance and testing for each Protection System device as requested by Reliability*First.* Additionally, Triton Power had documented maintenance and testing procedures but did not have those procedures summarized in its Program, as required.	To mitigate the issue, Triton Power revised its Program to include maintenance and testing intervals and their basis, as well as summaries of maintenance and testing procedures for all its Protection System devices.
Reliability*First* Corporation (Reliability*First*)	Triton Power Michigan, LLC (Triton)	NCR11174	RFC2012009965	PRC-005-1a	R2; R2.1	On February 14, 2012, Triton Power, as the Generator Owner for Jackson Power Company LLC, self-reported an issue with PRC-005-1 R2.1. Triton Power failed to perform maintenance and testing on two current differential relays (the Relays) within the five-year interval included in its Protection System maintenance and testing program (Program). The Relays protect transmission lines leaving the Triton Power facility. Triton Power believed its Transmission Owner (TO) performed maintenance and testing on the relays in connection with identical relays at the TO's end of the transmission lines. Upon discovering that the TO was not responsible for performing maintenance and testing on the Relays, Triton Power determined it had not performed the maintenance and testing on the Relays within the required interval.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. Triton Power's TO performed maintenance and testing within its interval on an identical set of relays at its substation. These identical relays have the ability to separate the Triton Power facility from the BPS. Additionally, Triton Power has redundant primary trip relays and back-up trip relays protecting its facility which Triton Power tested within its Program interval. Finally, upon performing maintenance and testing, Triton Power determined that the Relays would have performed appropriately if called upon during the duration of the issue.	To mitigate the issue, on February 14, 2012, Triton Power added the Relays to its tracking spreadsheet and conducted maintenance and testing of the Relays by February 28, 2012.
Reliability*First* Corporation (Reliability*First*)	Triton Power Michigan, LLC (Triton Power)	NCR11174	RFC2012010614	FAC-009-1	R1	During the Compliance Audit, conducted from April 30, 2012 to May 11, 2012, Reliability*First* determined that Triton Power, as a Generator Owner, had an issue with FAC-009-1 R1. Triton Power did not determine ratings for six transmission conductors, the collector bus, and an underground cable. Because Triton did not determine ratings for these devices, the lack of ratings was not consistent with Triton's Facility Ratings Methodology pursuant to FAC-009-1 R1. Reliability*First* initially determined this issue actually related to an issue with FAC-008-1 R1. Subsequently, Reliability*First* determined the appropriate Reliability Standard was not FAC-008-1 R1, but rather FAC-009-1 R1. Reliability*First* dismissed the tracking number associated with the issue with FAC-008-1 R1 (RFC201201613) and incorporated the facts of the issue with FAC-008-1 R1 as an issue with FAC-009-1 R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that the Triton Power facility was designed so that none of its generators could exceed the limitations of its associated electrical equipment. Triton Power's electrical equipment was designed with sufficient capacity to accommodate all the generators simultaneously operating at maximum output. Specifically, Triton Power cannot exceed the limitations of any of its electrical equipment since the electrical equipment was designed with sufficient capacity to accommodate the maximum output.	To mitigate the issue, Triton Power revised its Facility Ratings Methodology to include the missing components and also revised its overall Facility Ratings to reflect the most limiting element at the time all generation is leaving the facility.
Reliability*First* Corporation (Reliability*First*)	Wolverine Power Supply Cooperative, Inc. (Wolverine)	NCR00954	RFC2012010407	EOP-008-0	R1; R1.3	On May 16, 2012, Reliability*First* conducted a Compliance Audit of Wolverine. Reliability*First* determined that Wolverine, as a Transmission Operator, had an issue with EOP-008-0 R1.3. Specifically, Wolverine's contingency plan document, *Back-up Control Center Implementation Plan, revision 6* , dated December 30, 2011, failed to address the monitoring and control of critical transmission facilities, generation control, voltage control, time and frequency control, control of critical substation devices, and logging of significant power system events for loss of control center functionality.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). An issue with EOP-008-0 R1.3 has the potential to affect the reliable operation of the BPS by enabling a registered entity to have a deficient contingency plan in the event its control center becomes inoperable. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. Wolverine has a small transmission footprint with a single, looped 138 kV interconnection and does not have any critical transmission facilities. In addition, although Wolverine failed to specifically address each required element in EOP-008-0 R1.3, some of those elements were not applicable, and all others were indirectly addressed by an instruction in the *Back-up Control Center Implementation Plan* to validate that certain relays are working properly. As a result, the issue was documentary in nature and not reflective of a lack of contingency planning.	To mitigate the issue, Wolverine updated its *Back-up Control Center Implementation Plan* to specifically address each item in R1.3 and validated those changes with an operational run at its back-up control center.
Southwest Power Pool Regional Entity	Oklahoma Municipal Power Authority (OMPA)	NCR04108	SPP2012011463	PRC-008-0	R2; R2.1, R2.2	On November 30, 2012, OMPA, as a Distribution Provider, self-reported an issue with PRC-008-0 R2. Specifically, OMPA failed to test 7 of its 42 (16.67%) Under Frequency Load Shedding (UFLS) relays within the three-year interval defined in OMPA's PRC-008-0 R1 procedure. Of the seven relays that weren't tested within interval, the five relays located at Ponca City were not tested within the three-year interval due to a scheduling error by OMPA's testing consultants. The one relay located at Kingfisher was not tested because of the amount of load on the substation at the time OMPA was testing, precluded removing the UFLS relay from service. The one relay at OMPA's Pawhuska substation had not been tested because it had been removed from service.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Only 16.67% of the UFLS relays were tested out of OMPA's defined testing interval. Of the seven, the five relays located at Ponca City were tested less than one month past the three-year interval. The other two relays were tested within a year of the due date. Furthermore, OMPA's three-year interval for its UFLS relays is conservative because the NERC Technical Reference document recommends an interval of 10 years for testing UVLS or UFLS relays. Finally, the seven relays, combined, shed only 35.5 MW of OMPA's peak load of 736 MW and had frequency setpoints spread across the three frequency load shed points (59.3 Hz, 59.0 Hz, and 58.7 Hz).	OMPA tested the seven relays it had failed to test within the defined three-year interval, the five relays located at Ponca City were tested in January 2012, and the relay at Kingfisher was tested in November 2012. OMPA installed a relay, which had been tested on November 21, 2011, at Pawhuska on December 18, 2012. OMPA had tested these relays one year prior to installation. Additionally, after OMPA tested the Kingfisher relay, it replaced it with a spare relay, which had been tested on December 7, 2011. OMPA also updated its Protection System Maintenance Program (PSMP) and its NERC Procedure PRC-008 to change testing intervals from three years to six years to prevent reoccurrence. SPP RE verified completion of the mitigating activities.
Texas Reliability Entity, Inc (Texas RE)	EDF Trading North America, LLC (EDF Trading)	NCR00551	TRE2012009735	VAR-002-1.1b	R3	On February 13, 2012, EDF Trading, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3. EDT Trading stated that on February 1, 2012, a unit at the Altura Cogen Facility was out of automatic voltage control from approximately 21:34 p.m. to approximately 23:19 p.m. This was not reported to the Transmission Operator (TOP) within 30 minutes of the status change, as required by this Standard. After the warm-up of the unit, the plant board operator commenced ramping-up the unit at approximately 21:34 p.m., which is also when the operator observed unusual MW and MVAR flows. Immediately afterwards, the plant board operator contacted the on-call electrician to assess the situation. While the troubleshooting did not reveal any equipment defects, at about 23:18 p.m., it was discovered that the Voltage Regulator had shifted to manual. At that time, the Unit received a "Master Reset," which returned the Voltage Regulator to automatic.	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 corrected within one hour and 45 minutes. The incident occurred during a routine start-up of the unit that was providing 55 MW of power at the time. Also, the unit was still ramping-up and was not in Automatic Generation Control (AGC). Therefore, the unit had not been released to the Electric Reliability Council of Texas (ERCOT) economic dispatch control when the incident occurred.	EDF Trading has provided training to all on-site operators to monitor and detect changes in the status or capability of the Voltage Regulator, and updated the Emergency Operating Procedure to include these steps. The steps are identified as "immediate actions" when indications for possible Voltage Control issues appear. Texas RE has verified that the mitigation activities are complete.

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)	Colorado Energy Management - MPC (COMPC)	NCR10378	WECC2012011383	VAR-002-1.1b	R3	On November 9, 2012 and January 4, 2013, COMPC, as a Generator Operator, submitted Self-Reports citing issues with VAR-002-1.1b R3 and VAR-501-WECC-1 R1. According to the Self-Reports, on October 26, 2012, COMPC began a startup of its Gas Turbine 12. Upon startup, COMPC employees mistakenly informed its Transmission Operator (TOP) that the Power System Stabilizer (PSS) for Gas Turbine 12 was in service and active when, in actuality, the PSS had changed to manual mode and was inactive. After the unit had been online approximately eight hours, COMPC realized that the PSS was in manual mode and was not active or in service. COMPC reported that it switched the PSS to automatic mode and alerted its TOP of the status change as soon as it discovered that the PSS was in manual mode. COMPC reported, however, that it did not report the status change of the PSS to its TOP within 30 minutes of the change as required by VAR-002-1.1b R3.1. Furthermore, COMPC stated that as a result of its PSS being offline on October 26, 2012, the PSS was not in service for at least 98% of all operating hours in the fourth quarter of 2012. Specifically, COMPC noted that for the fourth quarter of 2012 the PSS should have been in service for 244.7 hours but was actually in service 235.9 hours or 96.4% of all operating hours.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In this instance, the risks to the reliability of the BPS were minimized by COMPC's compensating measures. During the duration of the issue, COMPC maintained its TOP's established voltage schedule. Additionally, the automatic voltage regulator attached to Gas Turbine 12 was in automatic mode and would have reacted appropriately if a change in voltage would have occurred. Furthermore, COMPC's other turbine units were equipped with an automatic PSS; these devices were available to respond in the appropriate manner and would have operated to prevent any damaging consequences that could have resulted from any increased voltage levels or reactive flows. Moreover, COMPC's internal procedures ensured that once the issue was discovered the TOP was immediately notified of the change and duration of the status change. Finally, COMPC serves only as a peaking plant at the direction of its TOP, thus if anything were to occur at the plant it would have minimal impact on the service of the TOP.	To mitigate this issue, COMPC: 1) retrained its employees on the importance and requirements of VAR-002-1.1b R3, specifically focusing on the requirement to report status changes within thirty minutes; and 2) reemphasized the procedures for handling and reporting status changes as required by VAR-002-1.1b. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Colorado Energy Management - MPC (COMPC)	NCR10378	WECC2013011658	VAR-501-WECC-1	R1	On November 9, 2012 and January 4, 2013, COMPC, as a Generator Operator, submitted two Self-Reports citing issues with VAR-002-1.1b R3 and VAR-501-WECC-1 R1. According to the Self-Reports, on October 26, 2012, COMPC began a startup of its Gas Turbine 12. Upon startup, COMPC employees mistakenly informed its Transmission Operator (TOP) that the Power System Stabilizer (PSS) for Gas Turbine 12 was in service and active when, in actuality, the PSS had changed to manual mode and was inactive. After the unit had been online approximately eight hours, COMPC realized that the PSS was in manual mode and was not active or in service. COMPC reported that it switched the PSS to automatic mode and alerted its TOP of the status change as soon as it discovered that the PSS was in manual mode. COMPC reported, however, that it did not report the status change of the PSS to its TOP within 30 minutes of the change as required by VAR-002-1.1b R3.1. Furthermore, COMPC stated that as a result of its PSS being offline on October 26, 2012, the PSS was not in service for at least 98% of all operating hours in the fourth quarter of 2012. Specifically, COMPC noted that for the fourth quarter of 2012 the PSS should have been in service for 244.7 hours but was actually in service 235.9 hours or 96.4% of all operating hours.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). In this instance, the potential risks to the BPS were minimized by COMPC's compensating measures. During the duration of the issue, COMPC maintained its TOP's established voltage schedule. Additionally, the automatic voltage regulator attached to Gas Turbine 12 was in automatic mode and would have reacted appropriately if a change in voltage would have occurred. Furthermore, COMPC's other turbine units were equipped with an automatic PSS; these devices were available to respond in the appropriate manner and would have operated to prevent any damaging consequences that could have resulted from any increased voltage levels or reactive flows. Moreover, COMPC's internal procedures ensured that once the issue was discovered the TOP was immediately notified of the change and duration of the status change. Finally, COMPC serves only as a peaking plant at the direction of its TOP, thus if anything were to occur at the plant it would have minimal impact on the service of the TOP.	To mitigate this issue, COMPC: 1) retrained its employees on the importance and requirements of VAR-002-1.1b R3, specifically focusing on the requirement to report status changes within thirty minutes; and 2) reemphasized the procedures for handling and reporting status changes as required by VAR-002-1.1b. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	El Paso Electric Company (EPE)	NCR05140	WECC2012009553	BAL-002-0	R4	From December 5, 2011, WECC conducted a Compliance Audit of EPE. BAL-002-0 R4 was not included in the NERC 2011 Compliance Monitoring and Enforcement Program (CMEP) Implementation Plan of Actively Monitored Standards; therefore it was not in the original scope of the Audit. During the course of the Audit however, the audit team's evaluations of EPE, as a Balancing Authority, resulted in the discovery of a possible Disturbance Control Performance issue. On June 18, 2010, a reportable disturbance occurred and EPE failed to activate the contingency reserves of the Southwest Reserve Sharing Group (SRSG) making EPE responsible for disturbance recovery for this event. Specifically, EPE did not recover its Area Control Error (ACE) until 22 minutes after the disturbance was issued. This disturbance took EPE seven minutes beyond the required Disturbance Recovery Period of 15 minutes to return its ACE to zero.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The event addressed herein represents an isolated case of EPE recovering its ACE seven minutes late. This resulted in EPE's Disturbance Control Standard (DCS) for the second quarter of 2010 being less than 100% because it had failed to recover from a single DCS reportable event within the allowable timeframe. Although EPE failed to recover its ACE within the 15 minute time limit, EPE only lost 101 MW of generating capability over a period of seven minutes. In addition, EPE did not experience an overload nor did the tie lines experience any voltage issues during the delay. Despite the recovery delay, the Reserve Sharing Group met the DCS requirement for more than 90% of the reportable disturbances.	To mitigate this issue, EPE: 1) EPE recovered its ACE 22 minutes from the initiation of the disturbance; and 2) EPE engaged in discussions with appropriate parties, including its reserve sharing group and the operator of the unit that tripped. The discussions between EPE and unit operator centered around the conduct of the operator on duty that day, and the discussions between EPE and the reserve sharing group administrator centered around the reserve sharing group Participation Agreement and its associated operating procedures governing disturbance reporting.
Western Electricity Coordinating Council (WECC)	PacifiCorp (PAC)	NCR05304	WECC2012011291	PRC-004-WECC-1	R1	On October 25, 2012, PAC, as a Transmission Owner, submitted a Self-Report citing an issue with PRC-004-WECC-1 R1. PAC disclosed that on three occasions it failed to analyze relay operations within 20 business days as required under R1.2. PAC disclosed that on July 23, 2012, two relays tripped on the Dillon Salmon Big Grassy 161 kV, WECC Path 18. PAC also disclosed that on July 28, 2012, there was another relay trip on the same line. PAC System Operators reviewed all three relay trips within 24 hours and determined that no misoperation occurred. System protection personnel did not review the three operations within 20 business days per R1.2. Rather, PAC system protection personnel analyzed the three operations on September 4, 2012. Operations that occurred on July 23, 2012, were reviewed after 31 business days. The operation on July 28, 2012, was reviewed after a lapse of 27 business days.	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 PAC's issue is, limited. Within 24 hours, PAC operators detected the relay trips and determined that there had been no misoperation. Further, protection system personnel did quickly analyze relay operations. Personnel determined there was no malfunction or equipment damage and that the relays had operated normally. This analysis, although late occurred seven to eleven days beyond the 20 day timeline described in R1.2.	To mitigate this issue, PAC: 1) analyzed the three relay operations; and 2) provided additional training to operational personnel regarding the proper response to relay operations including, but not limited to what parties are to be notified as well as tracking requirements. WECC has verified the completion of all mitigation activity.

Attachment A-2

February 28, 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 1 (NPCC_URE1)	NCRXXXXX	NPCC2012010874	CIP-004-3	R4; R4.1	NPCC_URE1 self-reported an issue with CIP-004-3 R4.1. NPCC_URE1 failed to update its list of personnel with authorized cyber access to Critical Cyber Assets (CCAs) within seven calendar days. NPCC_URE1 was informed by a vendor that one of its personnel with authorized cyber access to CCAs was no longer employed by the vendor. The employee had voluntarily resigned his position 32 days earlier and the vendor immediately revoked cyber access to all of NPCC_URE1's CCAs for the individual on the date of his termination. Because the vendor did not inform NPCC_URE1 of the employee's access revocation until 32 days had passed, NPCC_URE1's list was not updated within seven days.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). A personnel risk assessment (PRA) had been completed on the individual at issue prior to his being granted access to NPCC_URE1's CCAs. The PRA was still valid at the time of his resignation. The individual had also completed annual cybersecurity training, as required by NPCC_URE1's cybersecurity training program. The individual was never issued an identification card or access card by NPCC_URE1. This individual was never granted unescorted physical access to NPCC_URE1's CCAs. After the employee resigned, the vendor revoked all electronic access to NPCC_URE1 Cyber Assets. NPCC_URE1 has inspected the electronic access logs for NPCC_URE1's Electronic Security Perimeter and verified that the individual did not access any of NPCC_URE1's CCAs after the date of termination of his employment.	To mitigate this issue, NPCC_URE1 updated its protected cyber system access list to accurately reflect the status of all applicable personnel. NPCC_URE1 now requires that vendors and contractors notify NPCC_URE1 within 24 hours when the employment status changes for an individual with unescorted physical access or cyber access to NPCC_URE1's protected Cyber Assets. NPCC_URE1 updated its CIP annual training for vendors and NPCC_URE1 managers to include the review of specific requirements for removal of access and updating of access lists at the time of termination. NPCC_URE1 also revised the PRA section of its contract service agreements to include provisions requiring the vendor to notify NPCC_URE1 within 24 hours when unescorted physical access or cyber access is no longer required or the vendor terminates an employee. Lastly, NPCC_URE1 verified that applicable vendors have procedures to notify NPCC_URE1 within 24 hours when an applicable employee is terminated or there is a relevant change in the employee's status.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010753	CIP-004-1	R3	RFC_URE1 self-reported an issue with CIP-004-1 R3 to Reliability*First*. RFC_URE1 identified the issue as relating to CIP-006-1 R1.8. Reliability*First* subsequently determined that the facts and circumstances constituted an issue with CIP-004-1 R3. RFC_URE1 contracted with a consultant to conduct an annual review of its personnel risk assessment (PRA) program. As a result of that review, RFC_URE1 discovered three instances where it granted its employees authorized cyber access to Critical Cyber Assets without conducting a timely PRA. For two of the employees, RFC_URE1 granted cyber access before it completed the respective PRAs 10 months and 14 months later. For the third employee, RFC_URE1 granted cyber access seven days before the employee completed the PRA. In its Self-Report, RFC_URE1 identified seven additional instances where it granted cyber access to an employee prior to conducting a PRA. Reliability*First* determined, however, that these instances were not possible violations because CIP-004-1 R3 was in effect during the time period, which required RFC_URE1 to conduct a PRA within 30 days of granting cyber access. For the seven instances, RFC_URE1 conducted the PRA within 30 days of granting cyber access.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). A violation of CIP-004 R3 has the potential to affect the reliable operation of the BPS by providing the opportunity for unknown, unverified, or criminal individuals to access Critical Cyber Assets (CCAs), which could result in harm to the integrity of the CCAs. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. The individuals at issue were part of one of the following two user groups: service dispatchers and IT support. First, the service dispatchers have read-only access to the energy control system in a distribution operator capacity due to RFC_URE1's use of the energy control system for distribution in addition to transmission. Second, the IT support personnel had cyber access to workstations that are physical access control system assets where the IT support personnel only had operating system access and not application access. Operating system access allows the user to modify only the underlying operating system including device drivers and add or upgrade applications as required for support of corporate services. These individuals had no rights to the physical access control system and could not modify any access rights or privileges within that system. Application access requires an additional level of authentication that these individuals did not have.	To mitigate the issue, RFC_URE1: 1) reviewed the status of all individuals with authorized cyber or authorized unescorted physical access to CCAs; 2) verified that all individuals have current PRAs within seven years; 3) revised its procedures to review the daily report of employee change records to ensure appropriate access grants; and 4) revised its PRA verification procedures to ensure it conducts PRAs prior to granting access.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011578	CIP-005-1	R1; R1.6	Reliability*First* conducted a Compliance Audit of RFC_URE2. During the Compliance Audit, Reliability*First* determined RFC_URE2 did not maintain its documentation pursuant to CIP-005-1 R1.6. Specifically, RFC_URE2 did not synchronize all Electronic Security Perimeter (ESP) related documentation, did not document all Cyber Assets, did not clearly mark all electronic access points to the ESP, and did not categorize Cyber Assets as Critical Cyber Assets or access points.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that this issue was a documentation error. During Compliance Audit, Reliability*First* confirmed during a site visit that, although documentation was lacking, RFC_URE2 was properly protecting all of its Cyber Assets within an Electronic Security Perimeter and Physical Security Perimeter.	To mitigate the issue, RFC_URE2: 1) synchronized its documentation related to its ESP; 2) included and properly categorized all Cyber Assets; and 3) ensured its documentation clearly marked electronic access points to the ESP.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011579	CIP-007-1	R1; R1.3	Reliability*First* conducted a Compliance Audit of RFC_URE2. During the Compliance Audit, Reliability*First* determined RFC_URE2 did not document all test results for all change requests, as required by CIP-007-1 R1.3. RFC_URE2 uses a test script worksheet to process all change requests. Reliability*First* discovered several instances in which RFC_URE2 did not complete, or only partially completed, test scripts for change requests.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that this issue was a documentation error. This issue was a documentation error because, although RFC_URE2 did not fully document the test results, RFC_URE2 was able to demonstrate that it followed and successfully completed each step listed on its test script worksheet for all change requests.	To mitigate the issue, RFC_URE2 reinforced the requirement that test scripts must be completed for every change request and includes instructions on its test scripts stating, "a Pass or Fail must be entered on every step before form can be closed."
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011580	CIP-007-1	R3	Reliability*First* conducted a Compliance Audit of RFC_URE2. During the Compliance Audit, Reliability*First* determined RFC_URE2 had an issue with CIP-007-1 R3 as it did not document that it assessed security patches and security upgrades within 30 calendar days of availability. Reliability*First* also determined RFC_URE2 did not document the compensating measures it applied to mitigate risk exposure for those patches it did not install.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that this issue was a documentation error. During the Compliance Audit RFC_URE2 provided Reliability*First* with evidence demonstrating that it kept all its Cyber Assets up to date with the latest available patches even though RFC_URE2 did not document that it assessed security patches and security upgrades within 30 calendar days of availability.	To mitigate the issue, RFC_URE2 updated its security patch management procedure to help ensure it documents its assessment of security patches within 30 calendar days and documents the compensating measures it applies for those patches it does not install.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012011581	CIP-007-1	R6; R6.5	Reliability*First* conducted a Compliance Audit of RFC_URE2. During the Compliance Audit, Reliability*First* determined RFC_URE2 had an issue with CIP-007-1 R6.5 as it could not provide documentation that demonstrated it reviewed its system event logs.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that this issue was a documentation error. RFC_URE2 had system event logs, but it did not document its review of those logs. RFC_URE2 reviewed the logs but was unable to demonstrate its review of the logs. Additionally, the risk was mitigated by the fact that RFC_URE2's network is a closed network with no access to the Internet. Furthermore, RFC_URE2 generates alerts from its access points of events that could pose potential risk to the BPS.	To mitigate the issue, RFC_URE2 revised its monitoring and logging procedure to ensure that RFC_URE2 reviews and maintains records documenting the review of logs of system events related to cybersecurity at least quarterly.

Attachment A-2

February 28, 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
Reliability*First* Corporation (Reliability*First*); Texas Reliability Entity, Inc. (Texas RE); Southwest Power Pool Regional Entity (SPP RE) (collectively, the Regional Entities)	Unidentified Registered Entity 3 (RFC_URE3, TRE_URE3, SPP RE_URE3) (Collectively, URE_3)	NCRXXXXX	RFC2012009909 TRE2012009940 SPP2012009918	CIP-004-3	R4	This issue involved four incidents of noncompliance with CIP-004-3 R4 by URE_3: 1) URE3 self-reported an issue with CIP-004-3 R4 to three Regional Entities. A contractor in URE3's workplace services department, who had authorized unescorted physical access to Critical Cyber Assets (CCAs), resigned and no longer required such access. URE_3 failed to revoke the employee's access within seven calendar days as required by the Standard, and revoked the employee's access 30 days later; 2) URE_3 submitted a Self-Report to three Regional Entities identifying an issue with CIP-004-3 R4. The Self-Report identified one common instance of an issue among the Regional Entites and one additional instance unique only to SPP RE. Subsequently, URE_3 submitted evidence demonstrating that it did not in fact have an issue with CIP-004-3 R4 with respect to the common instance. As a result, the Regional Entities did not pursue this issue. However, the instance unique only to SPP RE was a non-compliant issue. URE3 submitted a Self-Report to SPP RE identifying an issue with CIP-004-3 R4. A building maintenance technician who had physical access to a Physical Security Perimeter resigned and no longer required such access. URE_3 failed to revoke the employee's access within seven calendar days, and revoked the employee's access nine days later; 3) URE_3's submitted Self-Reports to the Regional Entities identifying an issue with CIP-004-3 R4. An URE_3 employee within an operations business unit who had authorized cyber access to certain generation control supervisory control and data acquisition system CCAs no longer required such access. URE_3 failed to revoke the employee's access within seven calendar days, and revoked the employee's access 36 days later; and 4) URE_3 submitted Self-Reports to the Regional Entities identifying an issue with CIP-004-3 R4. An information technology service desk contractor who had authorized cyber access to CCAs no longer required such access. URE_3 failed to revoke the contractor's access within seven calendar days and revoked the contractor's access 18 days later.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). An issue with CIP-004 R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for personnel that a responsible entity determined should no longer have access to CCAs, with potential access to CCAs. Such continued access could result in harm to the integrity of the CCAs or the reliability of the BPS as a result of actions by an individual who should no longer have physical or electronic access to CCAs. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. URE_3 discovered these instances of noncompliance due to its internal controls when it performed its routine quarterly reviews of employees and contract employees. In each instance, URE_3 revoked access almost immediately after discovering it had not revoked access, and, in each instance, URE_3 discovered the issue no later than one month after access revocation was required. In addition, all of the employees and contractors in each instance were not terminated for cause and resigned except for one employee, whose manager determined that access was no longer required to perform the job function. Furthermore, the individuals who had physical access no longer had their physical access badges, reducing the likelihood the individuals could gain access to the Physical Security Perimeter. One individual did not have physical access at the time of resignation, and URE_3 collected that individual's secure identification token at the time of resignation thereby preventing remote access.	To mitigate the issue, URE_3: 1) revoked the individuals' access rights; 2) identified, developed, and made available awareness and training for managers who have NERC CIP contractors or employees; 3) sent a letter to managers summarizing termination responsibilities; 4) developed a pending revocation report to show all outstanding electronic access revocation requests; and 5) made appropriate clarifications on the form utilized to begin the process of terminating an individual's electronic access.
Reliability*First* Corporation (Reliability*First*); Texas Reliability Entity, Inc. (Texas RE); Southwest Power Pool Regional Entity (SPP RE) (collectively, the Regional Entities)	Unidentified Registered Entity 3 (RFC_URE3, TRE_URE3, SPP RE_URE3) (Collectively, URE_3)	NCRXXXXX	RFC2012001311 TRE2012009732 SPP2012009559	CIP-006-3c	R1; R1.4; R1.6	URE3 submitted respective Self-Reports to SPP RE, Texas RE, and Reliability*First* identifying an issue with CIP-006-3c R1.4. An URE_3 information technology (IT) employee without authorized unescorted physical access entered a Physical Security Perimeter (PSP) by tailgating through a door. The URE_3 IT employee entered the lobby adjoining the PSP. At 13:47, an URE_3 operations employee with authorized unescorted physical access exited the PSP door, and at the same time, the URE_3 IT employee exited the elevator and walked quickly toward the PSP door, grabbing the door handle just before the door closed and locked. The URE_3 IT employee pulled the door open, walked through it, and wandered around the floor before asking for assistance from an administrative assistant. The URE_3 IT employee was escorted to the electronic logging system, received a badge, and was checked in and out as a visitor. 9 minutes later, the URE_3 IT employee was escorted out of the area. URE_3 submitted Self-Reports to Reliability*First* and SPP RE identifying an issue with CIP-006-3c R1.6 which stemmed from three instances of noncompliance. First, an instance occurred that impacted Reliability*First* and SPP RE. URE_3 staff visited the an URE3 engineer for area development discussion. The discussion occurred in an URE_3 meeting room. During the meeting, the engineer briefly exited the meeting room for 15 to 20 seconds to go to the printer. The visitors remained in the room during this unescorted period because the meeting room, which is located down the hall from the printer, is visible from the printer area and the individual was only outside of the room for a few seconds to retrieve a printout. Second, an instance occurred that impacted Reliability*First* and SPP RE. A security guard escorted a vending machine repairman into control center kitchen to repair a vending machine. At an unknown point, the security guard left the repairman alone in the kitchen without transferring escort responsibility to control center personnel. The repairman remained in the kitchen until requesting the control center personnel to let the repairman exit the kitchen. The control center operator escorted the repairman to the main entrance of the control center where the security guard met them and resumed escort out of the center. Third, an instance occurred that impacted SPP RE only. URE_3 received an alarm indicating that a door was forced open at a supervisory control and data acquisition (SCADA) Computer Room main door. The operations center called the room and an URE_3 electrician answered the phone. The electrician reported that when he entered the room, he set the alarm off, and he could not exit the room. The operations center discovered that the electrician did not have the correct access for this room and opened the door for the electrician so he could exit the room. The operations center relocked the door once the electrician exited the room, and asked the electrician to pull on the door to ensure that it was locked. URE_3 conducted a follow-up investigation and discovered that the door magnetic lock was not fully engaged, but the door locks met close enough to show that the door was closed. Furthermore, URE_3 discovered that it had revoked the electrician's access to that room during quarterly access reviews when the electrician was on a leave of absence. The electrician still maintains authorized unescorted physical access to other areas. URE_3 submitted a Self-Report to Reliability*First* identifying an issue with CIP-006-3c R1.6. An URE_3 wireman had visitors at a substation in order to pull new cables into the substation. The wireman called the security department to request the ability to prop a door open at the substation in order to install the new cable runs in the substation. The security department granted the request and advised the wireman to swipe his badge each time he entered and exited the control house at the substation, and sign the visitors in and out each time they entered and exited the control house. The security department advised the wireman to call the security department every time the visitors entered and exited the control house as well and that the wireman should not leave the visitors unescorted in the control house. The security department received a door prop alarm from a door at the substation, as expected. A few hours later, the security department ran a badge analysis history for the wireman because the door had been propped open for several hours, and the security department had received no calls. Two hours later, the security department manager advised the security department to call the control house, at which time the wireman said that the visitors were still onsite and, at one point, the wireman went to his van leaving the visitors unescorted. As a result, URE_3 failed to provide these visitors with a continuous escort.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). An issue with CIP-006-3c R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to physically access Cyber Assets that are not protected by the implementation of a physical security plan. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. The issue occurred for a short duration prior to the URE_3 IT employee being logged in and escorted. In addition, at no time was the URE_3 IT employee in proximity to Critical Cyber Assets (CCAs) without an escort. Authorized personnel were in close proximity to the CCAs and would likely have resisted any unauthorized attempts at physical access. All of the escorting employees at issue remain employees of URE_3 who are trusted with authorized unescorted physical access. Regarding the instance where URE3 left meeting attendees unescorted for 15 to 20 seconds, the meeting room has no CCAs and there are multiple layers of security access control devices between the meeting room and the CCAs including a biometric reader, proxy card reader, and man-trap doors. In addition, the engineer attested that the visitors remained in the meeting room during the unescorted period. The visitors remained in the room during this unescorted period because the meeting room, which is located down the hall from the printer, is visible from the printer area and the individual was only outside of the room for a few seconds to retrieve a printout. Regarding the instance with the vending machine repairman, there are no CCAs in the kitchen. The CCA area is isolated and far away from the kitchen. There were six operators on duty in the CCA area during the unescorted period and no one saw the repairman leave the kitchen area until he was finished with the repairs. Regarding the instance with the electrician, the electrician had a valid personnel risk assessment and cybersecurity training. Until his leave of absence, he had authorized unescorted physical access to the computer room. CCAs are protected by username and password, and the Electronic Security Perimeter is protected by an access control list that verifies access rights. URE_3 had not assigned contractors usernames and passwords, so they could not access the CCAs.	URE_3 submitted to Reliability*First* a Mitigation Plan to address the issue with CIP-006-3c R1.4. URE_3 enhanced its physical barriers by installing keycard restrictions in the elevators through which the tailgater entered, requiring the use of a building badge for the elevator to stop at the lobby, and modifying the door to ensure it closes more quickly. In addition, URE_3 improved signage at the relevant location by performing an assessment of the existing signage and create and implement a strategy for enhancing existing signage. Furthermore, URE_3 provided additional training for personnel who have authorized unescorted physical access to the relevant PSP on the responsibilities of having such access, including ensuring that doors close securely during ingress and egress and monitoring the activities of individuals in the lobbies outside the PSP to prevent tailgating. URE_3 submitted to Reliability*First* a Mitigation Plan to address the issue with CIP-006-3c R1.6. URE_3 revised its communication and operation procedures to minimize human error including security awareness training, signage regarding visitors, minimizing visitors to the control center during off-business hours, and reminding escorts and visitors of the CIP requirements upon sign in. In addition, URE_3 reconfigured the operations center to remove the office area meeting room from the PSP, updated the operations center visitor check-in process, and repaired the SCADA room security door.
Reliability*First* Corporation (ReliabilityFirst)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012010100	CIP-006-3c	R1; R1.1	RFC_URE3 submitted a Self-Report to Reliability*First* identifying an issue with CIP-006-3c R1.1. While conducting annual preventative maintenance on its security system, RFC_URE3 discovered approximately seven 22 by 12 inch holes with cables running through them above the main door to a telecom room. Two weeks later, AEP repaired the holes. RFC_URE3 identified an addition instance of CIP-006-3c R1 in Reliability*First*. At a supervisory control and data acquisition (SCADA) computer room Physical Security Perimeter (PSP), RFC_URE3 discovered several instances where there was a 25 to 35 inch gap between the top of the walls and the concrete roof support. 2 weeks later, RFC_URE3 repaired the holes.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated because there are additional layers of security that one would have to penetrate to enter the PSP. The PSP is located in a small room within a larger room that has a separate door with a keypad lock. The holes did not lead outside the larger room. The SCADA computer room is located inside a building perimeter with partial fencing, and is secured with locks and card readers.	RFC_URE3 submitted to Reliability*First* a Mitigation Plan to address the first instance of the issue with CIP-006-3c R1.1. RFC_URE3 patched the gaps in the six-wall border and updated its physical security site survey checklist to remind services to: inspect rooms for potential gaps in the six-wall border; have workplace services and/or physical security personnel inspect all PSPs for any gaps in the six-wall border; review and inspect questionable gaps; and remediate any gaps discovered.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012001312	CIP-006-3c	R5	RFC_URE3 self-reported an issue with CIP-006-3c R5 to Reliability*First*. The station manager for a substation reported an issue to the security department. The station crew had permission to prop open the CIP station control building door while pulling in new control cables. At some point during their work, the crew began searching for materials in the station yard and left the control building unattended with the doors propped open for approximately 20 minutes. The station superintendent brought this to the crew's attention and reported the issue to the security deparment. RFC_URE3 failed to monitor these physical access point during that time period.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). An issue with CIP-006 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity to access the Physical Security Perimeter as failure to comply with the Standard means there are inadequate technical and procedural controls to monitor physical access points. The risk posed to the reliability of the BPS by the issue was mitigated by the following factors. RFC_URE3's station manager identified this issue and reported it immediately as a CIP issue to the security department, illustrating that RFC_URE3's internal controls caused RFC_URE3 to discover this issue. No unauthorized personnel were in the control house at the time the station superintendent re-entered it. The Critical Cyber Asset devices are protected by access control lists and require usernames and passwords in order to access the devices. In addition, the contractors were working outside in the yard approximately 1,000 feet from the control house. A supervisor was onsite and none of the contractors entered the building.	To mitigate the issue, RFC_URE3: 1) held a meeting with the associated station manager to discuss the mitigation options; 2) held a staff meeting with the department to review the CIP procedures for propping doors open for work; 3) developed a discussion training guide to reinforce the policy and expected conduct; 4) sent out an email reminder with the previous documents and summary; and 5) implemented a reminder script from the security department on the door prop open request for the security department to read to the station staff requesting the door prop.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012011126	CIP-002-1	R2	Reliability*First* conducted a Compliance Audit of RFC_URE4. During the Compliance Audit, Reliability*First* determined that RFC_URE4 did not have a documented risk-based assessment methodology (RBAM) to identify Critical Assets pursuant to CIP-002-1 R1. Therefore, RFC_URE4 could not demonstrate that it applied its RBAM annually to develop a list of Critical Assets pursuant to CIP-002-1 R2.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that RFC_URE4 has no Critical Assets. Throughout the duration of the issue, RFC_URE4 used a spreadsheet with evaluation criteria rather than a documented and approved RBAM to determine if it had Critical Assets. Examples of evaluation criteria RFC_URE4 used include whether an asset at issue is critical to initial restoration and automatic load shedding or functioned as a control center or back-up control center.	To mitigate the issue, RFC_URE4: 1) conducted a NERC Reliability Standard Compliance training program for RFC_URE4 personnel; 2) appointed a compliance coordinator; 3) confirmed it has no Critical Assets; and 4) approved a documented RBAM.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012011127	CIP-002-1	R4	Reliability*First* conducted a Compliance Audit of RFC_URE4. During the Compliance Audit, Reliability*First* determined RFC_URE4 did not have a documented risk-based assessment methodology (RBAM) to identify Critical Assets pursuant to CIP-002-3 R1. Therefore, RFC_URE4 could not demonstrate that it annually approved its RBAM pursuant to CIP-002-3 R4.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that RFC_URE4 has no Critical Assets. Throughout the duration of the issue, RFC_URE4 used a spreadsheet with evaluation criteria rather than a documented and approved RBAM to determine if it had Critical Assets. Examples of evaluation criteria RFC_URE4 used include whether an asset at issue is critical to initial restoration and automatic load shedding or functioned as a control center or back-up control center.	To mitigate the issue, RFC_URE4: 1) conducted a NERC Reliability Standard Compliance training program for RFC_URE4 personnel; 2) appointed a compliance coordinator; 3) confirmed it has no Critical Assets; and 4) approved a documented RBAM.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012011128	CIP-003-3	R2; R2.2	During a Compliance Audit. Reliability*First* determined that RFC_URE4 could not provide evidence that it documented a change to its senior manager designation within 30 calendar days of the effective date. Specifically, although RFC_URE4 appointed its plant manager as the senior manager for implementation of, and adherence to, the CIP Reliability Standards, RFC_URE4 failed to document this change within 30 calendar days.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that this was a documentation error. It was a documentation error because RFC_URE4 did appoint a senior CIP manager who functioned in that capacity throughout the duration of the issue. RFC_URE4 just neglected to document the change.	To mitigate the issue, RFC_URE4 appointed a senior manager and documented the change.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012011129	CIP-002-1	R1	Reliability*First* conducted a Compliance Audit of RFC_URE4. During the Compliance Audit, Reliability*First* determined that RFC_URE4 did not have a documented risk-based assessment methodology (RBAM) to identify Critical Assets pursuant to CIP-002-3 R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS by the issue was mitigated by the fact that RFC_URE4 has no Critical Assets. Throughout the duration of the issue, RFC_URE4 used a spreadsheet with evaluation criteria rather than a documented and approved RBAM to determine if it had Critical Assets. Examples of evaluation criteria RFC_URE4 used include whether an asset at issue is critical to initial restoration and automatic load shedding or functioned as a control center or back-up control center.	To mitigate the issue, RFC_URE4: 1) conducted a NERC Reliability Standard Compliance training program for RFC_URE4 personnel; 2) appointed a compliance coordinator; 3) confirmed it has no Critical Assets; and 4) approved a documented RBAM.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC200900651	CIP-004-1	R2	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-004-1 R2.1 because it had failed to establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCA). SERC_URE1 learned that a contractor for SERC_URE1's agent had access to CCAs for support and maintenance purposes but was unaware of specific CIP-004 requirements. While the contractor's firm maintained some cyber security training and awareness, these internal efforts did not cover specific entity policies and access controls, proper use of CCAs, proper handling of CCA information, plans to recover or re-establish CCAs, or documentation of training conducted. It was determined that SERC_URE1 did not have adequate procedures to monitor and ensure CIP-004 R2 compliance of personnel with access to CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue was for one contractor with only remote electronic access to memory devices. The untrained contractor only provided technical support for memory devices that supported CCA servers.	To mitigate this issue, SERC_URE1's agent implemented a cyber security training program that covered all aspects of CIP-004 R2.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC200900652	CIP-004-1	R3	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-004-1 R3 because it failed to have a documented personnel risk assessment (PRA) program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs). SERC_URE1 learned that a contractor for SERC_URE1's agent had access to Critical Cyber Assets (CCAs) for support and maintenance purposes but was unaware of specific CIP-004 requirements. While the contractor's firm performed some pre-employment background checks, these internal efforts did not meet the level required by CIP-004-1 R3. It was determined that SERC_URE1 did not have a PRA program that sufficiently addressed contractor personnel with access to CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue was for one contractor with only remote electronic access to memory devices. The contractor only provided support for memory devices that supported CCA servers.	To mitigate this issue, SERC_URE1's agent implemented a PRA program for contractors with access to CCAs.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC200900653	CIP-004-1	R4	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-004-1 R4 because it failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs), including their specific electronic and physical access rights to CCAs. SERC_URE1 learned that a contractor for SERC_URE1's agent had access to CCAs for support and maintenance purposes but was unaware of specific CIP-004 requirements. It was determined that SERC_URE1 did not include the contractor on its list of personnel with authorized cyber or authorized unescorted physical access to CCAs, including his or her specific electronic and physical access rights to CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue was for one contractor with only remote electronic access to memory devices. The contractor only provided support for memory devices that supported CCA servers.	To mitigate this issue, SERC_URE1's agent implemented an automated process for tracking contractors and employees with authorized cyber or unescorted physical access to CCAs.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC200900654	CIP-004-1	R4	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-004-1 R4 because it failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCA), including their specific electronic and physical access rights to CCAs. It was found that 19 employees of SERC_URE1's agent who had access to CCAs were reassigned and were not removed from the list within the allowed seven day revocation period for employees who no longer need access to CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All the missed individuals had valid and current personnel risk assessments and CIP cyber security training.	To mitigate this issue, SERC_URE1's agent implemented an automated process for tracking contractors and employees with authorized cyber or unescorted physical access to CCAs. This automated process also includes features that enable the removal of access within the timeframes specified by CIP-004 R4 .

Attachment A-2
February 28, 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	SERC200900655	CIP-005-1	R2	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-005-1 R2 because the firewall of SERC_URE1's agent was inadvertently configured to the "any-any" access rule, and was not set-up to deny access by default. It was determined that the firewall that formed the Electronic Security Perimeter (ESP) was installed prior to the date of mandatory compliance by SERC_URE1's agent and had a default access rule used for testing and trouble-shooting the pre-production system that was left intact once the system went into production. Pursuant to SERC_URE1 agent's ESP procedure, this rule should have been removed prior to the mandatory and effective date of CIP-005-1 R2; however, this rule replacement did not occur. During an evaluation of the ESP, SERC_URE1's agent discovered the overly permissive "any-any" access rule and initiated an internal investigation of all other ESP firewalls. SERC_URE1 agent's investigation concluded and SERC_URE1's agent removed the "any-any" rule and replaced it with a more stringent rule that denies access by default on this ESP firewall. No other instances of the permissive "any-any" rule were found on any ESP forming firewalls.	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 agent had a corporate firewall that had a deny-by-default access setting that had to be traversed in order to reach the ESP firewall. Only employees that had met the training and screening requirements of CIP-004 were allowed access through the corporate firewall, which is outside the ESP firewall.	To mitigate this issue, SERC_URE1's agent: 1) removed the non-compliant firewall and installed a CIP-005 R2 compliant firewall in its place; 2) determined if there were any other production ESP firewalls not in compliance with CIP-005 R2; 3) revised its procedures for ESP firewalls; and 4) notified SERC_URE1 that it completed training for the SERC_URE1 agent's employees working on CIP-005 R2.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000660	CIP-003-1	R3	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-003-1 R3 because it had been unable to perform personnel risk assessments (PRAs) on some of the individuals with access to Critical Cyber Assets (CCAs) due to a collective bargaining agreement (CBA) issue. Because of this, SERC_URE1 should have taken an exception to its cyber security policy (CSP), but it failed to do so. It was determined that, as of the date of mandatory compliance, SERC_URE1's agent had implemented a CSP but had not taken an exception to the CSP on the issue of PRAs for its union employees. SERC_URE1 agent's management realized that the CBA with its union employees did not allow for the performance of the PRA for those employees, and recognized this issue required an exception to the CSP that was never sought. SERC_URE1's agent obtained the authority to conduct PRAs on represented employees with access to CCAs. All required PRAs for the union employees were completed.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The exception to the CSP was only necessary because of a CBA that prevented the performance of PRAs for union employees. CIP-004 R3 explicitly notes that the requirement to perform PRAs for personnel with authorized access to CCAs is subject to existing collective bargaining unit agreements.	To mitigate this issue, SERC_URE1's agent completed all PRAs for union employees with access to CCAs.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000661	CIP-006-1	R1	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-006-1 R1 because it had not considered the application that monitors and controls the physical access to Physical Security Perimeters (PSPs) as a Cyber Asset, and all employees who used the system did not have valid personnel risk assessments (PRAs). It was determined that the subject of this Self-Report was a physical access control system (PACS) that managed physical access to Critical Cyber Assets (CCAs) and other secure areas not covered by the CIP standards. The PACS system was designed and segmented by permissions, so employees that managed PSPs were required to have PRAs and employees and contractors who managed non-CIP secure areas were not required to have PRAs since they could not access, manage, or control the PSPs. As understanding and knowledge of the CIP requirements regarding PACS increased, SERC_URE1 became aware that all employees with access to the PACS system should have valid PRAs and training.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The PACS system was set-up and segmented to prevent non-CIP users from being able to access the CIP designated PSPs. The PACS system is not directly tied to the Energy Management System.	To mitigate this issue, SERC_URE1's agent: 1) assembled a list of all personnel who had access to the security application that monitors and controls physical access to PSPs and processed PRAs for these employees and notified the manager upon completion of the PRAs; 2) determined if any other Cyber Assets or CCAs were not protected at the access point similar to the security application and reported its findings; 3) modified its cyber security policy and associated procedures to ensure that it is clear that all Cyber Assets and CCAs are protected at the access point; 4) modified its cyber security policy and associated procedures to require PRAs prior to granting an employee or contractor access to a Cyber Assets subject to CIP-006 R1.8; 5) trained all personnel, as applicable, on the revised procedures developed in items 3 and 4 above; and 6) revoked the access of any personnel who did not pass the PRA.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000662	CIP-007-1	R1	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-007-1 R1.1 because the test procedures did not specifically call out for tests of cyber security controls, but were instead focused on application and functional testing. It was determined that the test procedure did not address adverse effects to the production environment and were focused solely on application and functionality testing instead of also including specific instructions for testing cyber security controls.	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 agent addressed cyber security controls in its initial designs, and its change request process required a design document review in which security controls would be reviewed. Only documented and allowed traffic from outside the Electronic Security Perimeter (ESP) is permitted into the ESP.	To mitigate this issue, SERC_URE1's agent: 1) modified its testing procedures to explicitly include cyber security controls for significant changes in the test plan checklist; and 2) developed a training class on CIP-007 for all personnel responsible for the process of testing significant changes to ensure that the test plan checklist includes cyber security controls.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000663	CIP-007-1	R2	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-007-1 R2 because during a review of the ports and services documentation, operator workstations (which are Cyber Assets) within the Electronic Security Perimeter (ESP) were found to be missing from that initial compliance review. It was determined that SERC_URE1 had a procedure in place that detailed how to determine and document ports and services for each type of operating system in service as Critical Cyber Assets (CCAs) or non-critical Cyber Assets within the ESP. The original investigation between SERC_URE1 and SERC_URE1's agent determined that subparts of the procedure were violated, and ports and services for certain Cyber Assets within the ESP (the operator workstations) were not documented.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. These missing workstations were exclusively available to operators within the Physical Security Perimeter and ESP, where only permitted traffic is allowed, and were not accessible from outside the ESP. These workstations were located within the ESP, they were protected by anti-virus and current software patches and monitored in real-time by an intrusion detection system.	To mitigate this issue, SERC_URE1's agent: 1) determined if any other Cyber Assets within the ESPs were not compliant with CIP-007 and developed a plan to bring any such assets back into compliance; 2) trained all personnel responsible for change management process on the plan; and 3) completed all outstanding tasks from the plan.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000739	CIP-003-1	R1	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-003-1 R1.2 because it had failed to ensure the cyber security policy (CSP) of SERC_URE1's agent, was readily available to all personnel who had access to, or were responsible for, Critical Cyber Assets (CCA). SERC_URE1 learned that the CSP had not been provided to all contractors who had access to or were responsible for CCAs. This issue resulted from a lack of understanding that the contractors who had access to CCAs must also have ready access to the CSP. A copy of the CSP was later provided to the affected contract employees.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue -was limited to 12 contractors with remote electronic access. The contractors were from reputable companies that supported multiple cyber systems, so they were well aware of applicable cyber security controls.	To mitigate this issue, SERC_URE1's agent installed a computer kiosk at the entrance to the Electronic Security Perimeter with a copy of the SERC_URE1's agent's CSP to facilitate availability of the CSP for escorted personnel.

Attachment A-2
February 28, 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	SERC201000740	CIP-002-1	R3	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-002-1 R3 because it failed to identify certain workstations and laptops in its control center and back-up control center as Critical Cyber Assets (CCAs). SERC_URE1 learned that certain control centers and back-up control center workstations and laptops were not on its CCA list. The identified Cyber Assets that were deemed critical were added to the CCA list and all required CCA controls and protections were put into place.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. All workstations were protected by standard company security control practices for electronic and physical access. All workstations and laptops were located within the control center, a secure area.	To mitigate this issue, SERC_URE1's agent added each newly identified CCA to its official list.
Southwest Power Pool Regional Entity	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP2012009935	CIP-007-1	R5; R5.2.2	During a CIP Compliance Audit, SPP RE determined that SPP RE_URE1 was noncompliant with CIP-007-3 R5.2.2. Specifically, although SPP RE_URE1 had a documented list identifying individuals with access to shared accounts, the list did not include those individuals with access to one default shared local account for a Microsoft SQL Server database default account. This account is associated with a non-critical cyber asset located within the Electronic Security Perimeter (ESP), which is used solely as a historical data warehouse.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. SPP RE_URE1 only failed to document the individuals that had access to the shared local account for the Microsoft SQL Server database default account but the remaining individuals were identified correctly. Furthermore, the Microsoft SQL Server account only contained SPP RE_URE1 historical Energy Management System (EMS) data. The cyber asset did not have real-time capabilities; therefore any cyber security compromises to this asset would not have affected real-time operations. Finally, although undocumented, any individual who had access to the Microsoft SQL server would have had a documented Personal Risk Assessment (PRA) per SPP RE_URE1's access request and authorization process.	SPP RE_URE1 identified all individuals having access to the subject shared account and updated its shared user account list accordingly. SPP RE verified completion of the mitigating activities.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE2012009947	CIP-002-1	R1.2	During a Compliance Audit of Texas RE_URE1, Texas RE discovered an issue with Reliability Standard CIP-002-1 R1.2. Texas RE discovered that Texas RE_URE1 did not consider all assets listed in R1.2 when developing its risk-based assessment methodology (RBAM). Texas RE_URE1 had delegated certain function activities to a contractor but had failed to include the contractor's control center in its consideration of 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. After Texas RE_URE1 considered the contractor's facilities, Texas RE_URE1's list of Critical Assets or Critical Cyber Assets (CCA) remained null because the control center was deemed not to be a Critical Asset. The contractor does not perform any of the operations related to Texas RE_URE1's generation unit. The contractor is used as a communications medium between Texas RE_URE1's generation unit and other entities. Additionally, at the time of the issue, there was communication redundancy from the contractor to the plant that included four means of communication.	Texas RE_URE1 has included the contractor's control center as a consideration in its RBAM. The RBAM has been reviewed and signed by the current senior manager. Texas RE has verified the mitigation activities as complete.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) Horse Hollow Generation Tie, LLC (HHGT)	NCRXXXXX	TRE2012011389	CIP-002-3	R4	Texas RE_URE2 self-reported an issue with CIP-002-3 R4. Specifically, Texas RE_URE2 stated that it failed to follow its own procedures to have its risk-based assessment methodology (RBAM) and Critical Assets/Critical Cyber Assets (CCA) lists reviewed and signed annually by its CIP senior manager. Texas RE verified that Texas RE_URE2 did review its RBAM and Critical Assets/CCA lists in the prior year, and that the CIP senior manager responsible for signing the documents did so prior to the annual deadline. However, with the transition to a new CIP senior manager in the next year, Texas RE_URE2 failed to have these documents reviewed and signed by the annual deadline.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Once Texas RE_URE2 did review its RBAM, and its Critical Assets and CCA lists, no changes were noted. Therefore, Texas RE_URE2 had been operating with a complete list of Critical Assets/CCAs for the 12 days that the issue occurred.	Texas RE_URE2's new delegated CIP senior manager reviewed and signed the documents. Furthermore, to prevent reoccurrence, Texas RE_URE2 has implemented an automated notification system, which sends out notices to the appropriate personnel when the time for the annual review comes up. Texas RE has verified that these activities have been completed.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012011470	CIP-006-3c	R2	WECC_URE1 submitted a Self-Report to WECC citing an issue with CIP-006-3c R2. WECC_URE1 reported that it had been revising its risk-based assessment methodology (RBAM) and that based on the revised RBAM it was going to remove three facilities from its Critical Asset list. WECC_URE1 stated that prior to finalization of the new Critical Asset list, WECC_URE1 employees transferred certain Physical Access Control System (PACS) devices, which controlled access and logged information for the three facilities, from the PACS virtual local area networks (VLAN), which provides all of the protections required by CIP-006-3c R2.2, to the corporate security VLAN. WECC_URE1 noted that the corporate security VLAN does not provide all the requirements of CIP-006-3c R2.2. The PACS devices remained on the Corporate Security VLAN for four days until WECC_URE1's senior manager approved the new Critical Asset list removing the three facilities. WECC_URE1 reported that the PACS devices, which protected the facilities, were not afforded all of the protections required by CIP-006-3c R2.2. Specifically, when placed on the Corporate Security VLAN, WECC_URE1 failed to apply the protections afforded by CIP-003-3 R6, CIP-005-3 R2.4 and R2.5, CIP-006-3 R5, CIP-007-3 R1, and CIP-007-3 R7.2 and R7.3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risks posed by this issue were, to an extent, limited given the scope of the issue and compensating measures in place. The issue duration period is limited to four days, thus reducing vulnerabilities given the limited window of opportunity for possible intentional or unintentional misuse or intrusion. Further, the scope of the issue is limited to four PACS devices that were relocated to WECC_URE1's Corporate VLAN. WECC_URE1's Corporate VLAN is an isolated access network. Similar to an Electronic Security Perimeter (ESP), electronic access to the VLAN is controlled and monitored. Individuals who accessed the Corporate Security VLAN had completed Critical Infrastructure Protection training and a personnel risk assessment. Similarly, physical access to the PACS devices was controlled and monitored. Individuals with unescorted physical access completed training and were on the WECC_URE1's unescorted access list. The PACS devices were located within a Physical Security Perimeter (PSP). Furthermore, during the four day period, WECC_URE1 continued to log access to the PSPs containing PACS devices.	To mitigate this issue, WECC_URE1: 1) approved its revised RBAM and removed the three related facilities from its Critical Asset list; and 2) WECC_URE1 senior management discussed the issue and reiterated the importance of clear communications and Standard Owner responsibilities. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012010363	CIP-004-3	R4	WECC_URE2 submitted a Self-Report citing an issue with CIP-004-3 R4, specifically R4.1. WECC_URE2 reported that a telecommunications agent, who had authorized unescorted physical access to Critical Cyber Assets (CCAs) within the Physical Security Perimeter (PSP) located at WECC_URE2's system operations control center, was terminated from his position. WECC_URE2 noted that the individual did not have logical access to CCAs and was required to have physical access to the PSP as part of his job duties. WECC_URE2 reported that upon termination, the individual's access was revoked and his badge was collected by Human Resources but the personnel access list for CCAs was not updated to reflect the termination. WECC_URE2 stated that the assistant manager of system and trading operations discovered that the terminated individual no longer needed to be on the CCA authorized personnel list. On that same day, the assistant manager informed the personnel access list manager that the terminated employee no longer needed access to CCAs and the personnel access list manager subsequently deactivated the individual's physical access to the control system and removed the individual from the physical access list.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The risks posed by WECC_URE2's issue are, to an extent, minimized by the scope of the issue as well as compensating measures in place during the issue duration. The scope of the issue is limited to one employee. WECC_URE2 has procedures that include removing access badges and keys from employees after such employees have been terminated. Additionally, WECC_URE2 removes logical access to CCAs immediately upon termination. Furthermore, WECC_URE2 has a policy of training all employees who have access to CCAs and has all employees with such access undergo a personnel risk assessment (PRA). Moreover, the system control center is monitored by human observation 24 hours a day 7 days a week. Finally, in this case, WECC_URE2 revoked the employee's access and did collect the employee's access card (badge), thus precluding the employee from gaining access during pendency of the remediated issue and WECC_URE2 updated its access list within 11 days of the employee's departure.	To mitigate this issue, WECC_URE2: 1) updated the personnel access list and removed the terminated person from the list; 2) WECC_URE2's Human Resources department updated its notification and distribution process to include the system trading operations manager, personnel access list manager, and the system administrator to update the access list for personnel who no longer require access to CCAs as a result of separation actions; and 3) WECC_URE2's procedure for personnel access to CCAs was modified to include Human Resources and system trading operations manager notification. WECC 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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) Navajo Tribal Utility Authority (NTUA)	NCRXXXXX	WECC2012011000	CIP-002-2	R4	WECC performed an off-site Compliance Audit of WECC_URE3. During the Audit, the audit team concluded that WECC_URE3 had an issue with CIP-002-2 R4 for failing to have a CIP Senior Manager, or delegate thereof, sign and approve its risk-based assessment methodology (RBAM), its null list of Critical Assets, and its null list of Critical Cyber Assets (CCAs). WECC_URE3's general manager, who designated the CIP senior manager but is not the CIP designated senior manager or a delegate thereof, did approve WECC_URE3's RBAM, its null list of Critical Assets, and its null list of CCAs during the duration of the issue. In addition, WECC_URE3's CIP senior manager did sign an attestation documenting the annual dates on which he approved WECC_URE3's risk-based methodology, its null list of Critical Assets, and its null list of CCAs. The dates of the designated CIP senior manager's annual review and approval of WECC_URE3's risk-based methodology and the results of the assessment, which led to null lists of Critical Assets and CCAs, are identified in the attestation and align with WECC_URE3's other compliance documentation.	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, WECC_URE3's general manager had reviewed and approved its risk-based methodology, its null list of Critical Assets, and its null list of CCAs during the duration of the issue. Furthermore, there are documented emails from the CIP senior manager noting his awareness of the lists of Critical Assets and CCAs. The designated CIP senior manager reports directly or indirectly to the general manager. Accordingly, WECC_URE3 was aware that it did not have any Critical Assets or CCAs.	To mitigate this issue, WECC_URE3's CIP senior manager signed an attestation noting the annual dates on which he reviewed and approved its risk-based methodology, its null list of Critical Assets, and its null list of CCAs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012011468	CIP-004-3	R4	WECC_URE4 submitted a Self-Report citing an issue with CIP-004-3 R4. WECC_URE4 reported that it failed to revoke physical access to Critical Cyber Assets (CCAs) within seven days for an individual who no longer required such access. An individual employed by WECC_URE4 no longer required physical access to a single Physical Security Perimeter (PSP) containing CCAs. Per CIP-004-3 R4.3, access rights should have been revoked within seven days. Access was revoked within ten days.	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 WECC_URE4's issue is limited given the scope of the issue and the compensating measures in place during the duration of the issue. The individual maintained physical access rights to a single PSP for a period of three days beyond the period prescribed in R4.2. The individual in scope of the issue completed a personnel risk assessment, and cyber security training. The individual in scope did not attempt to physically access the CCAs. All of the CCAs to which the individual had access were contained within a Physical Security Perimeter. Physical access thereto was controlled and monitored. Unauthorized physical access attempts would have triggered alarming. The CCAs were also electronically secured within an Electronic Security Perimeter (ESP). Electronic access was controlled and monitored. Electronic access was limited to specific staff members who required such access. Cyber security events within the ESP containing the CCAs would have triggered alarming.	To mitigate this issue, WECC_URE4: 1) revoked individual's access to CCAs; and 2) implemented additional training and workload/resource management to prevent future instances of a similar nature.

Document Accession #: 20130228-5248 Filed Date: 02/28/2013

Document Content(s)