Federal Energy Regulatory Commission
Washington, D.C. 20426

Re:
Release Letter and Determination
Letter re: RC13-3
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 November 10, 2021, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC13-3, along with the names of one (1) relevant URE inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC13-3.

With respect to the remaining identities of UREs contained in RC13-3, 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 Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-

[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.

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 UREs associated with RC13-3 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: 2021.12.28 16:44:16 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

Document Accession #: 20121231-5257 Filed Date: 12/31/2012

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC13-3; - Optim Energy Altura Cogen, LLC (Optim) see .pdf page 26

December 31, 2012

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 25 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 44 possible violations[5] of 13 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 44 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 *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

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 DECEMBER 2012
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

FOR MRO:

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

Sara E. Patrick*
Vice President of Regulatory Affairs and Enforcement
Midwest Reliability Organization
380 St. Peter Street, Suite 800
St. Paul, MN 55102
(651) 855-1708
se.patrick@midwestreliability.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
December 31, 2012

Take notice that on December 31, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding twenty-five (25) 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

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*)	Ameren Energy Generating Company (AEGC)	NCR00677	RFC2011001176	PRC-005-1	R1	From July 11, 2011 to July 22, 2011, Reliability*First* conducted a Compliance Audit of AEGC, during which Reliability*First* discovered an issue with of PRC-005-1 R1. AEGC, as a Generator Owner, did not include maintenance and testing intervals for voltage and current sensing devices in its Protection System maintenance and testing program (Program) as required by PRC-005-1 R1.1. Although AEGC stated in its Program that it performed continuous monitoring as an alternative to defined intervals of maintenance and testing, Reliability*First* determined that AEGC's monitoring did not identify all types of instrument transformer failures and is therefore insufficient to qualify as an alternative to testing and maintenance intervals for those devices. As a result, AEGC's Program also failed to include a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. AEGC has in place an overall comprehensive maintenance and testing program, including partial continuous monitoring of instrument transformers with alarming, thermography, and commissioning testing. AEGC also conducts informal visual inspections of relays and instrument transformers. Lastly, no generating unit outage, equipment failure, or confirmation of any current and voltage sensing misoperation occurred during the period of the issue.	AEGC updated its Program to address the issue with PRC-005-1 R1. AEGC modified its Program, creating Revision 5 on September 14, 2012, to include a 12-year interval for load check and excitation tests on current sensing devices that were not subject to continuous monitoring.
Reliability*First* Corporation (Reliability*First*)	Ameren Energy Generating Company (AEGC)	NCR00677	RFC2011001177	PRC-005-1	R2; R2.2	From July 11, 2011 to July 22, 2011, Reliability*First* conducted a Compliance Audit of AEGC, during which Reliability*First* discovered an issue with PRC-005-1 R1. AEGC, as a Generator Owner, did not include maintenance and testing intervals for voltage and current sensing devices in its Protection System maintenance and testing program (Program) as required by PRC-005-1 R1.1. Although AEGC stated in its Program that it performed continuous monitoring as an alternative to defined intervals of maintenance and testing, Reliability*First* determined that AEGC's monitoring did not identify all types of instrument transformer failures and is therefore insufficient to qualify as an alternative to testing and maintenance intervals for those devices. As a result, AEGC's Program also failed to include a summary of maintenance and testing procedures for voltage and current sensing devices, as required by PRC-005-1 R1.2. In conjunction with the PRC-005-1 R1 issue, AEGC also failed to provide documentation of the date each voltage and current sensing device was last tested or maintained, as required by PRC-005-1 R2.2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. AEGC has in place an overall comprehensive maintenance and testing program, including partial continuous monitoring of instrument transformers with alarming, thermography, and commissioning testing. AEGC also conducts informal visual inspections of relays and instrument transformers. Lastly, no generating unit outage, equipment failure, or confirmation of any current and voltage sensing misoperation occurred during the period of the issue.	AEGC updated its Program to address the issue with PRC-005-1 R2. AEGC modified its Program, creating Revision 5 on September 14, 2012, to include a 12-year interval for load check and excitation tests on current sensing devices that were not subject to continuous monitoring. In addition, the responsible personnel were informed of the revision to the Program.
Reliability*First* Corporation (Reliability*First*)	Calumet Energy Team, LLC (Calumet)	NCR00252	RFC2011001094	PRC-005-1	R2	From July 11, 2011 to July 22, 2011, Reliability*First* conducted a Compliance Audit of Calumet, during which Reliability*First* discovered an issue with PRC-005-1 R2. Calumet, as a Generator Owner, did not provide Reliability*First* with documentation demonstrating that voltage and current sensing devices, direct current (DC) control circuitry, and protective relay devices were maintained and tested within defined intervals, as required by PRC-005-1 R2.1. Specifically, Calumet did not provide complete documentation to evidence testing of voltage and current sensing devices because the device designations from the prior test cycle are different than, and could not be correlated with, the device designations from the current records. Additionally, Calumet Energy did not provide any prior test records for DC control circuitry. Finally, Calumet Energy did not provide a test record relating to one protective relay.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although, for certain devices, Calumet failed to maintain proper documentation, it did conduct scheduled testing and maintenance for protective relays and voltage and current sensing devices. Additionally, although Calumet did not perform functional testing on DC control circuitry prior to 2010, it did verify continuity and functionality of trip circuits during normal unit shutdowns.	Calumet implemented a planned maintenance activity for performing DC circuitry testing to ensure that testing is performed in addition to the relay calibration tests. Calumet also developed appropriate designations for voltage and current sensing devices and matched those designations with the one-line diagram to ensure that all voltage and current sensing devices are tested and documented. Calumet Energy provided evidence of its updated preventative maintenance schedule for DC circuitry and updated documentation showing a clear correlation between test data for voltage and current sensing devices and the same devices on one-line diagrams.
Reliability*First* Corporation (Reliability*First*)	Delmarva Power & Light Company (Delmarva)	NCR00752	RFC2012011122	PRC-008-0	R2	On September 18, 2012, Delmarva, as a Distribution Provider, self-reported an issue with PRC-008-0 R2 to Reliability*First*. Delmarva did not maintain test results to demonstrate that it tested a distribution microprocessor relay with an under frequency load shedding (UFLS) scheme within the time frame specified in Delmarva's PRC-008-0 *Protective System Schemes Protection and Maintenance Program & Procedures* (Procedures). Specifically, Delmarva's Procedures require that it trip test UFLS microprocessor relays every eight years with a 10% grace period (9.6 months). Delmarva has evidence that it trip tested the relay on March 4, 2003 as part of the relay installation process. Based on the Procedures, the relay should have been trip tested again no later than December 21, 2011. In addition, Delmarva has spreadsheets showing the relay was trip tested on March 4, 2007, before the December 21, 2011 testing due date, but Delmarva was unable to locate test results evidencing the March 4, 2007 trip test.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The relay in question represents less than 1% of Delmarva's UFLS equipment. If Delmarva had experienced an under frequency excursion, it has sufficient UFLS equipment to meet the required load shedding without this relay. The relay was set to trip at the 58.9 Hertz (Hz) frequency level, which is the second set point in Delmarva's UFLS program. At this set point, Delmarva had planned to be able to shed 15.1% of its estimated annual peak load, even though its UFLS program only required it to shed 10% of its estimated annual peak load. Even if the relay had not operating correctly, Delmarva still would have been able to shed 13.7% of its estimated annual peak load. Similarly, if the relay had experienced a false trip, it only would have tripped one distribution circuit with 20 MW of load at peak. Additionally, the relay is a self-monitoring microprocessor relay and is therefore designed to alert operators if it fails. During the time period of the issue, the relay issued no alarms. Furthermore, the relay functioned as expected throughout the period in question and the July 31, 2012 trip test results confirm that the relay was functioning as intended. Prior to performing the trip test, a health check was performed and the report shows that the relay was functioning. During the time period of the issue, the multipurpose distribution relay correctly tripped for faults which tested the trip circuit and proved that the trip circuit was properly functioning. The relay did not experience any under frequency false trips during the time period of the alleged violation. Furthermore, there were no system under frequency events that required the UFLS function in the relay to operate during the period in question. Finally, this was an isolated incident that was discovered during a compliance activity, which Delmarva routinely conducts to ensure that it performs testing pursuant to its Procedure.	Delmarva trip tested the relay on July 31, 2012, the day after the discovery of this potential discrepancy, while a search for evidence continued. The July 31, 2012 test confirmed that the relay was functioning as intended. After completing the relay test, Delmarva reviewed its documentation for all UFLS equipment and determined that it had appropriate testing documentation for all other relays. Delmarva had also already implemented procedures to ensure that it performed testing per the Procedure. Furthermore, Delmarva already routinely conducted compliance activities to ensure that it performs testing pursuant to its Procedure.
Reliability*First* Corporation (Reliability*First*)	GenOn East 2	NCR11145	RFC2011001133	PRC-005-1	R2; R2.1	On September 30, 2011, GenOn East 2, as a Generator Owner, self-certified an issue with PRC-005-1 R2. GenOn East 2 failed to perform maintenance and testing on one of its 85 relays within the defined interval of four years (plus a 10% grace period). GenOn East 2 tested this relay, the backup relay for a primary relay, at a different time than the rest of the relays. GenOn East 2 did, however, maintain and test the primary relay within its defined interval.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The relay at issue is a backup relay for a primary relay that GenOn East 2 did maintain and test within its defined interval. The primary relay responds in a shorter timeframe to an event than the backup relay, and there are alarms in place that alert the control room when the devices operate or misoperate. In addition, GenOn East 2 discovered this issue while conducting a self-assessment. The issue occurred for approximately three months, and GenOn East 2 timely discovered and corrected this issue.	To address the issue, GenOn East 2 performed maintenance and testing on the relay at issue. GenOn revised its Protection System maintenance and testing program, which will aid to prevent recurrence.
Reliability*First* Corporation (Reliability*First*)	GenOn Power Midwest	NCR11136	RFC2012010406	VAR-002-1.1b	R1	On May 30, 2012, GenOn Power Midwest, as a Generator Operator and Generator Owner, self-reported an issue with VAR-002-1.1b R1 to Reliability*First* . On April 11, 2012, GenOn Power Midwest started its Brunot Island Unit 4 with the automatic voltage regulator (AVR) in manual mode. GenOn Power Midwest operated this unit in manual mode for approximately 29 hours, from April 11, 2012 through April 13, 2012, without notifying the Transmission Operator that the AVR was in manual mode.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. GenOn Power Midwest has a program in place requiring operation of the AVR in automatic mode, and there is alarming on Units 2, 3 and 4 for the AVR status. This instance, therefore, was an isolated occurrence. GenOn Power Midwest maintained the voltage schedule for Brunot Island during the time period of the issue and was aware that the AVR was in manual mode.	GenOn Power Midwest completed the following mitigating actions: 1) added a specific alarm for the AVR not operating in automatic mode; 2) reviewed current station operating procedures as well as the NERC compliance procedure and addressed any gaps; and 3) provided further training on VAR-002-1.1b and GenOn internal compliance procedures with plant personnel.

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*)	GenOn REMA 1	NCR11141	RFC2012010745	VAR-002-1.1b	R2	On July 9, 2012, GenOn REMA 1, as a Generator Operator and a Generator Owner, self-reported an issue with VAR-002-1.1b R2 to Reliability*First* . During a self-assessment, GenOn REMA 1 discovered that for its Sayreville and Werner generating stations, it failed to maintain generator voltage schedule without an exemption from the Transmission Operator on certain occasions. The Sayreville generating station consists of four combustion turbines totaling 224 MW, and the Werner generating station consists of four combustion turbines totaling 212 MW. On December 15, 2011 and December 21, 2011 the Werner station experienced voltage schedule excursions where the voltage was higher than the schedule. The Werner station was only operating two of its generating units at the time of the excursions. On December 23, 2011, February 21, 2012, March 2, 2012, and March 3, 2012, the Sayreville station experienced voltage schedule excursions where the voltage was slightly above or slightly below than the schedule. On each of those dates except February 21, 2012, the Sayreville station was only operating one of its generating units at the time of the excursions. On February 21, 2012, the Sayreville station was only operating two of its generating units at the time of the excursion. The greatest voltage excursion was only 1.13% above the voltage schedule.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The greatest voltage excursion was only 1.13% above the voltage schedule. In addition, the Automatic Voltage Regulators were in automatic mode during each of the voltage excursions.	GenOn REMA 1 completed the following mitigating actions: 1) initiated a review of the self-assessment incident findings with all employees, conducted training classes and review of VAR-002 requirements with all operators; 2) installed laminated guidelines on all dedicated voltage monitoring screens; 3) installed voltage schedule monitoring screens in all control rooms; and 4) updated operating start-up/shut-down check-off sheets to include the voltage schedule.
Reliability*First* Corporation (Reliability*First*)	NedPower Mount Storm, LLC (Ned Power)	NCR00293	RFC2012010024	PRC-005-1	R2; R2.1	On April 3, 2012, NedPower, as a Generator Owner, self-reported an issue with PRC-005-1 R2.1 to Reliability*First.* In preparation for an upcoming audit, NedPower conducted a review of its Reliability Standards compliance documentation for, among other Reliability Standards, PRC-005-1. During the review, NedPower discovered that it did not maintain evidence that it conducted two monthly battery inspections. From April 30, 2012 to May 16, 2012, Reliability*First* conducted a Compliance Audit of NedPower. Reliability*First* discovered additional facts related to NedPower's issue with PRC-005-1 R1. Specifically, NedPower did not maintain evidence that it performed visual inspections or heat scans for current and voltage sensing devices, as required within its Protection System maintenance and testing program (Program). Additionally, NedPower did not maintain evidence that it tested its control circuitry as required within its Program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NedPower missed two monthly battery inspections, with all remaining inspections immediately before and after each missed inspection demonstrating sufficient battery functioning and identifying no issues with the batteries. NedPower also performed a load test in August 2009 that showed no issues with the batteries. Additionally, NedPower's batteries and battery control house were installed in Fall 2007, with climate control in the control house, thereby protecting the batteries against degradation that would have limited their effectiveness. Furthermore, the batteries are monitored through continuous automatic alarms and regulator operator checks. In terms of its current and potential sensing devices, although NedPower missed the visual and heat scan inspections, NedPower did perform electrical testing on these devices when it performed the relay testing and NedPower would have discovered any problems with the devices during this testing.	NedPower completed the following mitigating actions: 1) addition of an additional layer of automation and protection to the compliance program to ensure that it completes monthly battery inspections; 2) implementation of a verification process to ensure that records of conducting heat scans are documented, signed, and dated; and 3) documentation of its verification that the control circuitry operational checks pass inspection and retains signed and dated verification sheets.
SERC Reliability Corporation (SERC)	City of Springfield, IL – CWLP (CWLP)	NCR01328	SERC2012009691	PRC-005-1	R1; R1.1; R1.2	On February 2, 2012, in preparation for a SERC audit, CWLP discovered an issue with its Generator Battery Maintenance Program for Dallman Unit 4. On February 9, 2012, CWLP, as a Generator Owner, self-reported an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program did not include maintenance and testing intervals and a summary of maintenance and testing procedures for the Dallman Unit 4 generator battery. The Self-Report also stated that Dallman Unit 4 entered commercial operation on November 20, 2009. SERC reviewed CWLP's Protection System maintenance and testing program and determined that CWLP's Protection System maintenance and testing procedures for station batteries did not include the battery testing and maintenance program for Dallman Unit 4 until February 9, 2012. SERC confirmed that CWLP's maintenance and testing procedures for its Transmission Owner and Distribution Provider functions had no issues.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1) Although the Dallman Unit 4 battery system was not included in CWLP's Protection System maintenance and testing procedure prior to February 9, 2012, CWLP maintained and tested the Unit 4 battery system in accordance with the same procedure it used to maintain and test the Unit 3 battery system which called for monthly and semi-annual testing of the Unit 3 batteries; and 2) After the Unit 4 battery system was included in CWLP's Protection System maintenance and testing procedure, CWLP tested the Unit 4 battery system in accordance with the updated procedure and found no problems, indicating that the battery system likely would have performed as intended.	SERC verified that CWLP completed the following actions: 1) Confirmed that the battery and maintenance testing intervals for the Dallman Unit 4 generator battery have been entered into the new MAXIMO system to ensure compliance with the current CWLP generator battery maintenance program; 2) Incorporated the Dallman Unit 4 generator battery into the CWLP generator battery maintenance program document and added language to the document requiring an annual review by CWLP generation personnel. The review will be coordinated with the CWLP Compliance Committee Chairman and the CWLP Chairman assigned responsibility for maintaining compliance with PRC-005; and 3) Updated the current contract with the vendor performing battery and maintenance testing as described in the CWLP generator battery maintenance program to include the Dallman Unit 4 generator battery.
SERC Reliability Corporation (SERC)	City of Springfield, IL – CWLP (CWLP)	NCR01328	SERC2012009692	PRC-005-1	R2; R2.1; R2.2	On February 2, 2012, in preparation for the SERC Compliance audit, CWLP discovered an issue with its Generator Battery Maintenance Program with Dallman Unit 4. On February 9, 2012, CWLP, as a Generator Owner, self-reported an issue with PRC-005-1 R2, stating that it did not have evidence that one generator battery system was maintained and tested within the defined intervals, and did not provide the date when the battery was last tested and maintained. The Self-Report also stated that Dallman Unit 4 entered commercial operation on November 20, 2009. SERC reviewed spreadsheets prepared by CWLP that included each of CWLP's Protection System devices and the defined maintenance and testing intervals, the most recent test date and the previous test date for each device. SERC verified the assigned intervals based on a review of CWLP's Protection System maintenance and testing procedure and determined that CWLP could not provide records of the last maintenance or testing date for one out of 13 station batteries (7.7%). In total, CWLP failed to have maintenance or test records for one out of 1,054 Protection System devices (0.1%).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1) CWLP has local and control room alarms on its battery systems that would alert CWLP personnel of a problem; 2) Although the Dallman Unit 4 battery system was not included in CWLP's Protection System maintenance and testing procedure prior to February 9, 2012, CWLP maintained and tested the Unit 4 battery system in accordance with the same procedure it used to maintain and test the Unit 3 battery system which called for monthly and semi-annual testing of the Unit 3 batteries; and 3) After the Unit 4 battery system was included in CWLP's Protection System maintenance and testing procedure, CWLP tested the Unit 4 battery system in accordance with the updated procedure and found no problems, indicating that the battery system likely would have performed as intended.	SERC verified that CWLP completed the following actions: 1) Confirmed that the battery and maintenance testing intervals for the Dallman Unit 4 generator battery have been entered into the new MAXIMO system to ensure compliance with the current CWLP generator battery maintenance program; 2) Incorporated the Dallman Unit 4 generator battery into the CWLP generator battery maintenance program document and added language to the document requiring an annual review by CWLP generation personnel. The review will be coordinated with the CWLP Compliance Committee Chairman and the CWLP Chairman assigned responsibility for maintaining compliance with PRC-005; and 3) Updated the current contract with the vendor performing battery and maintenance testing as described in the CWLP generator battery maintenance program to include the Dallman Unit 4 generator battery.

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)	City of Springfield, IL – CWLP (CWLP)	NCR01328	SERC2012009985	FAC-009-1	R1	On March 29, 2012, CWLP, as a Transmission Owner, self-reported an issue with FAC-009-1 R1, stating that an engineer discovered a transposition error regarding the winter emergency rating in its Facility Rating for a transmission conductor. CWLP stated that a transposition error was made in a summary table after the calculation of the equipment ratings was completed. The transposition error affected the winter emergency ratings on nine branches on the CWLP 138 kV transmission system. The winter emergency rating was incorrectly listed as 1,373 Amps instead of the correct value of 1,337 Amps, a difference of 36 Amps (2.62%). SERC reviewed the CWLP Facility Rating Methodology (FRM) and ratings summary spreadsheets dated before and after the self-reported event. The spreadsheets included a calculation of conductor rating, which was calculated to be 1,337 Amps for CWLP's 795 thousand circular mills (MCM) Aluminum Conductor Steel Reinforced (ACSR) transmission conductors. The summary table in the same spreadsheet contained manually entered values for the Facility Ratings rather than the calculated values, wherein the tens and unit digits were erroneously transposed, resulting in a stated transmission line rating of 1,373 Amps, instead of 1,337 Amps as was calculated. CWLP listed the incorrect conductor rating in the spreadsheet dated October 18, 2011 and corrected the conductor rating in the spreadsheet dated April 25, 2012. SERC reviewed data sheets used to transmit Facility Ratings to the entities requesting that data and found that CWLP determined and distributed a normal summer, normal winter, emergency summer, and emergency winter rating for 60 facilities, for a total of 240 Facility Ratings. Only the winter emergency ratings for nine facilities were affected by the manual input error. SERC determined that CWLP failed to establish nine out of 240 Facility Ratings (3.75%) for its solely and jointly owned facilities in a manner consistent with its FRM. SERC also reviewed CWLP's generation Facility Rating documents and confirmed that the issue does not apply to the Generator Owner function of CWLP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1) CWLP has a supervisory control and data acquisition (SCADA) system in place which provides an alarm to the system operator when the facility loading is at 90% of summer normal and winter normal ratings. This alarm provides sufficient time for CWLP to take action to prevent the load from approaching the emergency limits; 2) The affected facilities have never been included in the list of MISO Interconnection Reliability Operating Limit, Transmission Operator congested flow gates, or Critical Facilities List, and the facilities have never been identified by the CWLP vulnerability and risk assessment as a critical facility; and 3) After CWLP correctly applied the FRM to determine the Facility Ratings, the nine facilities' capacity rating was reduced by 2.62% for the winter emergency rating.	SERC verified that CWLP completed the following actions: 1) Coordinated the ratings change between the CWLP Compliance Chairman and the CWLP Operations engineer on March 20, 2012; 2) Implemented the ratings change with MISO Operations by using the web based modeling tool on March 20, 2012; 3) Received confirmation from MISO via email that the ratings had been updated in the MISO Real Time Model on March 20, 2012; 4) Coordinated the initiation of the change in the MISO Model on Demand (MOD) database between the CWLP Compliance Chairman and CWLP Planning on March 20, 2012, and submitted the change on March 22, 2012 due to the MISO MOD availability; and 5) Revised the CWLP Transmission Ratings Review Procedures to require that schedule calculations be performed to confirm that the correct ratings are being provided to CWLP Operations and CWLP Planning.
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner, (Gardner)	NCR10190	SPP201100622	FAC-008-1	R1	During a June 8, 2011 to June 9, 2011 Compliance Audit, the SPP RE Audit Team determined that Gardner, as a Transmission Owner, was noncompliant with FAC-008-1 R1. Between December 20, 2007 and June 10, 2010, Gardner did not have an established Facility Ratings Methodology (FRM), and between June 10, 2010 and June 9, 2011, Gardner's FRM failed to address the ratings of its current transformers (CTs).	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Gardner is a municipal electric utility with a peak load of 39.6 MW. It owns 3.6 miles of 161 kV transmission line, two 161 kV interconnections with its Transmission Operator (TOP) at one substation (Moonlight Substation), and no Bulk Electric System generation. The Moonlight Substation is jointly owned by Gardner and its TOP. Except for the feeds to Gardner, the TOP owns the remainder of the substation and the ties to the BPS. The Gardner system has minimal impact on flows through the Moonlight Substation, and therefore minimal impact on the surrounding BPS. The TOP has identified the ratings of equipment in the Moonlight Substation, and notwithstanding the lack of a Gardner FRM, the TOP is aware of the ratings of the Gardner facilities for planning purposes.	As of June 9, 2011, Gardner has established a FRM, which it will maintain and revise as needed.
Southwest Power Pool Regional Entity (SPP RE)	Exelon Wind 4, LLC (Exelon)	NCR10122	SPP2012010552	PRC-005-1	R2	During a June 25, 2012 Compliance Audit of Exelon, the SPP RE Audit Team identified noncompliance with PRC-005-1 R2. Exelon, as a Generator Owner, could not provide evidence that it conducted annual testing on one battery bank during 2010, nor could it provide evidence of monthly battery inspections for the months requested by the SPP RE Audit Team. The Audit period covered October 31, 2007 to June 25, 2012.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Exelon is a 79.8 MW wind facility that sells non-firm power. Exelon demonstrated that all its PRC-005 devices, except its battery bank, were tested and maintained within intervals defined in its Protection System maintenance and testing program. The single annual battery testing failure occurred in 2010, and Exelon provided evidence of battery testing for 2011, which showed no battery degradation. Furthermore, Exelon's battery bank is monitored and will alert inspection personnel of battery voltage issues. Although Exelon could not provide evidence of monthly battery inspections, it provided evidence that its inspection personnel conducted monthly inspections of the facilities where the battery bank was located.	Exelon performed maintenance and testing of its batteries in accordance with its maintenance and testing program in September 2011, and has revised the testing and inspection records to ensure documentation of monthly inspections and annual testing of its battery bank.
Southwest Power Pool Regional Entity (SPP RE)	Flat Ridge Wind Energy, LLC (Flat Ridge)	NCR10312	SPP2012010127	VAR-002-1.1b	R2; R2.2	Flat Ridge, as a Generator Operator, self-certified noncompliance with VAR-002-1.1b R2.2 on April 30, 2012 because of its inability to comply with its Transmission Operator's (TOP) voltage schedule. Flat Ridge's TOP provided it with a voltage schedule of 139 kV +/- 4 kV at the point of interconnection (POI) from December 17, 2009 through March 3, 2011 and a voltage schedule of 138 kV +/- 7 kV at the POI from March 3, 2011 through May 1, 2012. On April 27, 2012, Flat Ridge was notified by its new TOP that it would be required to adhere to a voltage schedule of 139 kV +/- 4 kV as of May 1, 2012. The new TOP directed Flat Ridge to "comply at all times, while the generator is on line, with the [new] Voltage Schedule and operate with the Automatic Voltage Regulator (AVR) in service and controlling voltage to maintain a constant voltage output at the interconnection point." Following notification of the new voltage schedule and while conducting a compliance review for the aforementioned self-certification, Flat Ridge identified voltage schedule deviations outside of its mandated voltage schedule, the majority of which were less than 1 kV, which occurred between December 17, 2009 and April 30, 2012. Flat Ridge was previously unaware of the deviations from the TOP's voltage schedule and had not notified its TOP that the deviations had occurred. Subsequently, Flat Ridge determined that it was unable to comply with the new TOP's voltage schedule due to facility limitations. The Flat Ridge wind facility relies on a tap changing transformer and a shunt capacitor bank control system for dynamic voltage control. These devices were determined to be incapable of maintaining the facility's voltage within 139 kV +/- 4 kV at all times.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). By design, the Flat Ridge wind facility's generators absorb reactive power and are incapable of contributing any substantial voltage support to the BPS. Finally, the majority of the voltage schedule excursions deviations by Flat Ridge were less than 1 kV and presented a minimal risk to the TOP's transmission system.	Flat Ridge coordinated a change with its TOP for a voltage schedule of 139 kV +/-4 kV to 141 kV +4/ -6 kV. This provided a voltage range that was sustainable given the wind facilities' design restrictions. Flat Ridge commissioned a third-party engineering analysis of its facility to determine if its capacitors could be modified to adhere to a tighter voltage range. The engineering study determined that the capacitors were correctly set for voltage priority, and that the devices were already configured properly to maintain the POI voltage within required limits. Flat Ridge also drafted and implemented a procedure to detect and notify its TOP of voltage deviations outside the newly established voltage range, and detailed mitigating activities that should be undertaken by operations personnel to remedy voltage schedule deviations.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Lafayette Utilities System (LAFA)	NCR01114	SPP2011008215	EOP-008-0	R1.6	During a September 19, 2011 to September 22, 2011 Compliance Audit of LAFA, the SPP RE Audit Team discovered noncompliance with EOP-008-0 R1.6. LAFA's contingency plan called for all of LAFA's personnel to receive annual training in the plan. However, the Audit Team determined that LAFA could not demonstrate that three out of five of its operators actually received annual training for loss of the primary control center in 2009 and 2010. This remediated issue applies to LAFA's Balancing Authority and Transmission Operator functions.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). LAFA did have a contingency plan in place during 2009 and 2010, and the Audit Team determined that the plan addressed the requirements of EOP-008-0, except for R1.6. Although LAFA could not demonstrate that three of its five operators had received annual training on the contingency plan, LAFA's system operators have been with LAFA for over five years and have had training on LAFA's contingency plan, including participating in drills, prior to 2009. All operators have had recent training on LAFA's contingency plan after 2010.	In order to assure that all LAFA operators complete site specific training for the loss of the primary control center in the future, LAFA scheduled its training in the following manner for each upcoming year: 1) Scheduled classroom instruction and discussion on the LAFA procedure as part of the operator's bi-monthly meeting in the first quarter of each year; 2) Scheduled each operator to perform the drill for the loss of the primary control center during the first quarter of each year on a date when there is no conflict with contracted training for certification hours. Should an emergency occur in the LAFA system or BES that requires the delay of this drill, it will be performed after the emergency has ceased on the next workday for the scheduled operator; 3) Added a field to its Training Tracking Tool for a requirement of completion of loss of primary control center training and updated to indicate that this training is required for the operators; and 4) Implemented an audit process and flagging and monitoring for this requirement in the LAFA Training Tracking Tool. Included classroom instruction and drills for the Loss of the Primary Control Center in the annual training plan for operators. Copies will be distributed to each operator and the supervisor in December of each year. Any time a change occurs in an employee training schedule, they are notified. Supervisors are sent monthly updates.
Southwest Power Pool Regional Entity (SPP RE)	Lea Power Partners, LLC (LEAPP)	NCR10301	SPP2012009184	FAC-009-1	R1	On January 17, 2012, LEAPP, as a Generator Owner, self-reported noncompliance with FAC-009-1 R1. LEAPP stated that it had not previously established the facility rating for its Hobbs Generating Station in accordance with its Facility Ratings Methodology (FRM). LEAPP had adopted a FRM calling for it to establish the Hobbs Generating Station Facility Rating by considering the individual ratings of the equipment comprising the station, ambient conditions, operating limitations and other factors. However, in application of its FRM, LEAPP had identified its Facility Rating as the "Net Capability" of the generating station, as identified in its Power Purchase Agreement (PPA) and identified the most limiting element of the Hobbs facility as the combustion turbine generators. LEAPP's PPA is not a factor in the determination of the facility rating of the Hobbs generating station and the most limiting elements of the facility are the step-up transformers for the combustion turbine and steam turbine generators.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although LEAPP had not developed the rating of the Hobbs facility based on its FRM, in practice, LEAPP operated the Hobbs units at their maximum capacity based upon operating limitations and ambient conditions. The maximum capacity rating, which LEAPP initially used, was more limiting than the actual nameplate rating. Accordingly, the operating capacity of the Hobbs generating facility was known to its Transmission Operator, Balancing Authority and Reliability Coordinator. Moreover, the Facility Rating of the Hobbs facility did not appreciably change once LEAPP's FRM was applied.	LEAPP reviewed and revised its site's Facility Rating to ensure the correct determination was presented on the summary page. LEAPP updated its Facility Rating to reference actual equipment limitations based upon name plate data or specification sheets when name plate data was not available. This review and revision was complete on January 17, 2012.
Southwest Power Pool Regional Entity (SPP RE)	Midwest Energy, Inc. (Midwest)	NCR01118	SPP2012009972	PRC-005-1	R2; R2.1	On March 30, 2012, Midwest, as a Distribution Provider and a Transmission Owner, self-reported noncompliance with PRC-005-1 R2.1. The Midwest Protection System Maintenance and Testing Procedure (PSMP) required the testing of station battery banks to occur within a five-year interval. Midwest determined that eight (34.8%) of its 23 station battery banks had not been tested within the five-year interval. Five of the battery banks exceeded the required testing date by three months or less. The remaining three battery banks exceeded the testing interval by two to 3.5 years. All of the identified battery banks had been tested as of April 3, 2012. On April 19, 2012, Midwest supplemented its original Self-Report of PRC-005-1 R2.1 with a letter describing a failure to test three (0.4%) of its 715 Protection System relays within the three-year interval prescribed by the Midwest PSMP. Midwest indicated that these microprocessor-based relays were tested upon commissioning in February 2008 but were not tested again until April 23, 2012, which is one year and two months beyond the prescribed interval.	SPP RE determined the remediated issues posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The three microprocessor-based relays were subject to monthly visual inspections and were constantly monitored by the Midwest Supervisory Control and Data Acquisition System (SCADA) for failure. Additionally, testing of the three relays occurred within four years and two months of the previous tests. This testing period was shorter than the recommended seven to 10 year testing interval identified in the NERC Protection System Maintenance Technical Reference (NERC Reference) for monitored microprocessor based relays. The station battery banks were also subject to monthly inspections that included corrosion checks, jumper contact checks, and the recording of battery charger DC voltage. Additionally, battery bank voltage is constantly monitored via Midwest's SCADA system. In this case, testing occurred at 5.25 years, 7 years, and 8.5 years, which falls within the maximum ten-year testing interval identified in the NERC Reference for monitored battery banks. No equipment failures resulted from the missed battery or relay testing intervals.	Midwest conducted testing on all battery banks exceeding the five-year testing interval and tested the three relays exceeding the three year-testing interval by April 23, 2012. Midwest also implemented electronic reminders to ensure staff is notified of pending equipment testing deadlines.
Texas Reliability Entity, Inc (Texas RE)	American Electric Power Service Corp as agent for AEP Texas North Co, AEP Texas Central Co, and Public Service of Oklahoma (AEP)	NCR04006	TRE2012010885	EOP-008-0	R1; R1.3; R1.7	During a August 10, 2012 Audit, it was discovered that AEP, as a Transmission Operator (TOP), did not include a list of critical transmission facilities in its control center contingency plan, as required by EOP-008-0 R1.3. In addition, AEP did not perform an annual review and update of its control center contingency plan in 2011, as required by R1.7. Texas RE determined the duration of this remediated issue to be from May 4, 2010, when AEP was registered as a TOP, to September 16, 2012, when AEP conducted an annual review of its control center contingency plan and included a list of critical transmission facilities in it.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). With respect to the instance of noncompliance with EOP-008-0 R1.3, Texas RE determined that AEP's control center contingency plan addressed the monitoring and control of all AEP transmission facilities. However, the plan was missing a list of facilities that were being monitored and controlled as critical or otherwise. During the Audit, it was confirmed that AEP had a list of critical transmission facilities that should be considered and addressed in the contingency plan but failed to include the list in its plan. Therefore, Texas RE considered this instance of noncompliance to be documentation related. With respect to the instance of noncompliance with EOP-008-0 R1.7, Texas RE determined that the risk to the BPS was minimal because AEP's plan was reviewed and updated within a 14 month period and no material changes were made after the review.	AEP took immediate action to correct this remediated issue and updated its control center contingency plan. The plan now includes the location where the critical facilities list can be accessed. The annual review and update of AEP's plan is now being tracked in a document control process to ensure the annual requirement is met. This issue was mitigated on February 28, 2012. Texas RE has verified the mitigation activities as complete.
Texas Reliability Entity, Inc (Texas RE)	Texas Medical Center Central Heating and Cooling Services Corp (TECO)	NCR11116	TRE2012011048	CIP-001-2a	R1	On August 28, 2012, TECO, as a Generator Owner, self-reported a remediated issue with CIP-001-2a R1 because TECO's previous company procedures did not fulfill the requirements for the recognition of and for making operating personnel aware of sabotage events. Texas RE determined the duration of this remediated issue to be from October 1, 2011, when TECO was required to comply with this Standard, to August 2, 2012, when TECO updated its sabotage reporting procedure to include recognition of and making operating personnel aware of sabotage events.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because TECO's generation unit is 48 MW and a potential failure of this generator would present a minimal risk to the BPS due to the low amount of power supplied. Approximately 80% of the MWh generated by TECO are consumed within TECO's Private Use Network (PUN). Finally, TECO did have security procedures in place prior to August 2, 2012; however, they did not address the specific requirements of CIP-001-2a R1. TECO's prior procedures had instructions to inspect grounds and report suspicious activity and included bomb threat emergency and acts of violence emergency and had instructions to notify operating personnel identified by title. Therefore, TECO's personnel was prepared to act if a sabotage event occurred.	TECO took actions to correct this remediated issue and executed an updated sabotage reporting procedure, which includes: 1) definitions for recognizing suspected sabotage events and responses for each; and 2) provisions for making operating personnel aware of sabotage events. Texas RE has verified the mitigation activities as 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
Texas Reliability Entity, Inc (Texas RE)	Texas Medical Center Central Heating and Cooling Services Corp (TECO)	NCR11116	TRE2012011049	CIP-001-2a	R3	On August 28, 2012, TECO, as a Generator Owner, self-reported an issue with CIP-001-2a R3 because TECO did not provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events. Texas RE determined the duration of this remediated issue to be from October 1, 2011, when TECO was required to comply with this Standard, to November 19, 2012, when TECO provided the updated sabotage reporting procedure to all operating personnel.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because TECO's generation unit is 48 MW and a potential failure of this generator would present a minimal risk to the BPS due to the low amount of power supplied. Approximately 80% of the MWh generated by TECO are consumed within TECO's Private Use Network (PUN). Finally, TECO did have security procedures in place prior to August 2, 2012; however, they did not address the specific requirements of CIP-001-2a R1. TECO's prior procedures had instructions to inspect grounds and report suspicious activity and included bomb threat emergency and acts of violence emergency and had instructions to notify operating personnel identified by title. Therefore, TECO's personnel was prepared to act if a sabotage event occurred.	TECO took action to correct this remediated issue and provided its updated sabotage reporting procedure to current operating personnel and included the procedure in new personnel training. Texas RE has verified the mitigation activities as complete. Additional sabotage awareness training is also scheduled by TECO.
Western Electricity Coordinating Council (WECC)	Central Arizona Water Conservation District (CAWC)	NCR05060	WECC2012010810	INT-004-2	R2	On August 1, 2012, CAWC submitted three Self-Reports citing possible noncompliance with INT-004-2 R2. Specifically, CAWC reported that on three occasions CAWC traders failed to update tags pursuant to INT-004-2 R2, sub-requirements R2.1 and R2.2. CAWC is registered in the NERC Compliance Registry as an entity performing the function of a Purchasing-Selling Entity. On February 29, 2012, the average energy profile for Navajo Generation was prescheduled at 364 MW. At 22:00 a Navajo unit was forced offline due to an unplanned outage. Although actual hourly interchange deviated from the hourly average energy profile by more than (-) 10%, CAWC did not update eight tags for the next available scheduling hours, HE24 through HE10. On May 7, 2012, a trader instructed the Navajo Generation Plant to ramp down to a level below the day-ahead planned interchange schedule. Consequently, the actual Navajo output for May 7, 2012, HE19 through HE24 deviated from the average hourly energy profile by more than 25 MW. On May 24, 2012, at 17:03, CAWC received notification of a planned outage of Navajo Unit 1 between 22:00 on May 25, 2012, and 14:00 on May 26, 2012. CAWC traders failed to update three Dynamic Interchange tags in anticipation of the planned outage. This failure resulted in the loss of 183 MW of resources used to serve load and excess sales. Further, traders failed to identify the Dynamic Interchange Schedule deviations and adjust the corresponding Dynamic Interchange tags for future hours during the planned outage. WECC's subject matter experts determined that, given the circumstances described in R2.1 and R2.2, CAWC failed to update a total of 12 tags on three occasions. WECC Enforcement also determined that in each of the three instances in which tags were not updated, traders acting on behalf of CAWC failed to follow established procedure that required tagging updates. WECC Enforcement dismissed possible violations WECC2012010811 and WECC2012010812 as separate enforcement actions. WECC Enforcement, therefore, determined to include the full scope of CAWC noncompliance with INT-004-2 R2 in a single enforcement action.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). INT-004-2 R2 requires Purchasing-Selling Entities to ensure that tags are updated for the next available scheduling hour and future hours under circumstances described by R2.1, R2.2 and R2.3. Failure to update the tags may cause potential loading voltage instability. In this case, CAWC failed to update 12 tags under the circumstances described by sub requirements R2.1 and R2.2. Human error was the cause of the noncompliance in each of the three instances in which CAWC failed to update tags. Traders acting on behalf of CAWC failed to follow established rules and procedures that required tagging updates per INT-004-2 R2. In each instance, CAWC was aware of the status of generation plant interties and load profiles in real-time through SCADA. Further, CAWC had an hourly load profile for each load location. The tags were limited to those associated with the hourly load profile of the Navajo generation unit. In each instance, CAWC would have been able to ramp up generation at other locations to compensate for the generation shortage at Navajo and prevent loading voltage instability to the system as a whole. WECC, therefore, determined that CAWC noncompliance with INT-004-2 R2, a remediated issue, posed a minimal risk to the BPS.	CAWC completed the following action by December 5, 2012, to remediate noncompliance with INT-004-2 R2: 1) CAWC implemented completed INT-004-2 retraining for CAWC staff and traders acting on behalf of CAWC; and 2) the two responsible traders were released from employment effective on June 21, 2012, and July 14, 2012, respectively.
Western Electricity Coordinating Council (WECC)	Dynegy Power, LLC (DYN)	NCR00200	WECC2012010759	VAR-002-1.1	R2	On July 9, 2012 DYN, as a Generator Operator and as a Generator Owner, submitted a Self-Report regarding a potential issue with VAR-002-1.1b R2. On July 23, 2012, DYN submitted a Self-Certification, which incorporated the Self-Report, reporting potential noncompliance with VAR-002-1.1b R2. In the Self-Certification, DYN reported that on June 6, 2012 one of its generators was operating at a higher terminal voltage than its Transmission Operator (TOP) target level allows. DYN reported that its TOP required its generators to operate at a voltage of 21.7 kV plus or minus 0.2 kV. In this instance, the DYN Operation Technician failed to adjust the power factor for two hours following the end of startup of the generator. DYN reported that for those two hours the generator was operating at a voltage which was 0.5 kV higher than its TOP's target levels. DYN noted that the operator recognized that the generator was operating at a voltage above the TOP's target level and adjusted the generator voltage to a voltage which is within the target level of its TOP. On July 18, 2012, a WECC Subject Matter Expert (SME) contacted DYN to discuss its Self-Report and Self-Certification. The SME determined that DYN had a possible issue with VAR-002-1.1b R2 for failing to operate its generators in accordance with its TOP's target levels. The SMEs determined, that for two hours on June 6, 2012, DYN operated one of its generators at a voltage level above the target levels set by its TOP. WECC Enforcement (Enforcement) reviewed DYN's Self-Report, Self-Certification, and the SME's findings. Enforcement determined that DYN had an issue with VAR-002-1.1b R2 because it allowed its generator to operate at a higher voltage level than that specified by its TOP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). DYN had a specific policy in place to prevent violations of VAR-002-1.1b. DYN had provided this information to its operators and the operators acted in accordance to this procedure. Following the procedure, DYN quickly resolved the issue once it was discovered. During the two hour time frame the TOP did not notice any changes in voltage in their system and did not contact the entity regarding the voltage output. Accordingly, WECC determined that this remediated issue posed a minimal risk to the BPS.	The issue was resolved when DYN's operation technician adjusted the voltage levels of the generator to comply with the TOP's target levels. DYN also submitted and completed a mitigation plan that required DYN to review its past voltage records to ensure compliance with VAR-002-1.1b R2, conduct a training session to refresh its employees in its procedures, and installed-an alarm that is intended to remind the operator to adjust generator voltage when the unit reaches 32 MW. The actual completion date of the mitigation activities was October 17, 2012.
Western Electricity Coordinating Council (WECC)	GenOn California I (GCAI)	NCR11148	WECC2012010731	VAR-002-1.1	R1	On July 20, 2012, GCAI, as a Generator Operator, submitted a Self-Certification citing possible noncompliance with VAR-002-1.1b R1. Specifically, GCAI reported that on May 31, 2012, at 08:43 AM, Etiwanda Unit 4 (Unit 4) was brought online in "manual" operating mode. Per standard operating procedure, the Automatic Voltage Regulator (AVR) at Unit 4 should trigger once the generator reaches a minimum load point. In this case, however, GCAI reported that at approximately 08:50 AM, Unit 4 reached the minimum load point, but that the AVR did not activate. Rather, Unit 4 remained in "manual" operating mode until 09:30 AM. GCAI made its Transmission Operator (TOP) aware that the unit was offline and that GCAI was planning on re-starting the unit. At 09:30 AM GCAI switched Unit 4 to AVR operating mode and notified its TOP of the change in Unit 4's operating status (specifically, that it switched from manual mode to AVR mode). WECC Subject Matter Experts (SMEs) reviewed GCAI's Self-Certifications and contacted the entity to request additional information. SMEs determined that on May 31, 2012, between 08:50 and 09:30 AM, GCAI failed to operate in AVR mode. SMEs forwarded their findings to WECC Enforcement (Enforcement). Enforcement reviewed GCAI's Self-Certifications and the SMEs' findings. Enforcement determined that per VAR-002-1.1b R1 entities are required to operate in AVR. In this case, Enforcement determined that between 08:50 and 09:30 AM, GCAI failed to operate Unit 4 in AVR. The TOP expected the unit to come online with the AVR in service controlling voltage. Enforcement, therefore, determined that GCAI had issues with VAR-002-1.1b R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). AVR operation is necessary to ensure that generation automatically adjusts for varying voltage levels and reactive flows on the BPS. Failure of a Generator Operator to operate in AVR may cause system disturbances with voltage variation. In this case, GCAI failed to operate Unit 4 in AVR for a period of approximately 40 minutes. Unit 4 comprises one out of a total of three units in service at Etiwanda. The other two units were operating in AVR, and were available to respond to voltage variation at the interconnection during the 40 minute period in which AVR at Unit 4 was disabled. During the 40 minute period in which Unit 4 AVR was not in operation, GCAI maintained the voltage schedule set by its Transmission Operator. Further, Unit 4's operating status was detected by GCAI dispatch at 08:50 AM. GCAI Generator Operators were notified and AVR was switched on by 09:30 AM. Enforcement, therefore, determined that GCAI**'s** noncompliance with VAR-002-1.1b R1 posed a minimal risk to the BPS.	On September 24, 2012, GCAI completed the following action to remediate noncompliance with VAR-002-1.1b R1 and R3: GCAI added AVR alarming to make its operating personnel aware of changes in status. GCAI revised its Start-up Checklist to include the following: 1) a requirement to ensure that the AVR is in-service; and 2) a requirement to ensure that the Power System Stabilizer (PSS) is in-service. GCAI added E-Alert notification for plant management regarding the operating status of AVR and PSS. To avoid future instances of possible noncompliance with VAR-002-1.1b R1 and R3, GCAI provided training on the modified start-up checklist for all plant operators.

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)	GenOn California I (GCAI)	NCR11148	WECC2012010734	VAR-002-1.1b	R3	On July 20, 2012, GCAI, as a Generator Operator, submitted a Self-Certification citing possible noncompliance with VAR-002-1.1b R3. Specifically, GCAI reported that on May 31, 2012, at 08:43 a.m., Etiwanda Unit 4 (Unit 4) was brought online in "manual" operating mode. Per standard operating procedure, the Automatic Voltage Regulator (AVR) at Unit 4 should trigger once the generator reaches a minimum load point. In this case, however, GCAI reported that at approximately 08:50 a.m., Unit 4 reached the minimum load point, but that the AVR did not activate. Rather, Unit 4 remained in "manual" operating mode until 09:30 a.m. GCAI made its Transmission Operator (TOP) aware that the unit was offline and that GCAI was planning on re-starting the unit. At 09:30 a.m GCAI switched Unit 4 to AVR operating mode and notified its TOP of the change in Unit 4's operating status (specifically, that it switched from manual mode to AVR mode). WECC Subject Matter Experts (SMEs) reviewed GCAI's Self-Certifications and contacted the entity to request additional information. SMEs determined that on May 31, 2012, between 08:50 and 09:30 a.m., GCAI failed to operate in AVR mode. Further, SMEs determined that GCAI's failure to notify the TOP of Unit 4's manual operating status between 08:50 and 09:30 a.m. was not in compliance with VAR-002-1.1b R3. SMEs forwarded their findings to WECC Enforcement (Enforcement). Enforcement reviewed GCAI's Self-Certification and the SMEs' findings. Enforcement determined that per VAR-002-1.1b R3, entities are required to notify the TOP within 30 minutes of a change in status of a reactive resource, including AVR. In this case, Enforcement determined that between 08:50 and 09:30 a.m. GCAI failed to operate Unit 4 in AVR. The TOP expected the unit to come online with the AVR in service controlling voltage. Enforcement also determined that GCAI failed to notify the TOP of its operating status within 30 minutes, or by 09:20 a.m. Enforcement, therefore, determined that GCAI had an issue with VAR-002-1.1b R3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). AVR operation is necessary to ensure that generation automatically adjusts for varying voltage levels and reactive flows on the BPS. Failure of a Generator Operator to operate in AVR may cause system disturbances with voltage variation. In this case, GCAI failed to operate Unit 4 in AVR for a period of approximately 40 minutes. Unit 4 comprises one out of a total of three units in service at Etiwanda. The other two units were operating in AVR, and were available to respond to voltage variation at the interconnection during the 40 minute period in which AVR at Unit 4 was disabled. During the 40 minute period in which Unit 4 AVR was not in operation, GCAI maintained the voltage schedule set by its Transmission Operator. Further, Unit 4's operating status was detected by GCAI dispatch at 08:50 a.m. GCAI Generator Operators were notified and AVR was switched on by 09:30 a.m. Enforcement, therefore, determined that GCAI noncompliance with VAR-002-1.1b R3 posed a minimal risk to the BPS.	On September 24, 2012, GCAI completed the following action to remediate noncompliance with VAR-002-1.1b R1 and R3: GCAI added AVR alarming to make its operating personnel aware of changes in status. GCAI revised its Start-up Checklist to include the following: 1) a requirement to ensure that the AVR is in-service; and 2) a requirement to ensure that the Power System Stabilizer (PSS) is in-service. GCAI added E-Alert notification for plant management regarding the operating status of AVR and PSS. To avoid future instances of possible noncompliance with VAR-002-1.1b R1 and R3, GCAI provided training on the modified start-up checklist for all plant operators.

Attachment A-2

December 31, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012010993	CIP-006-3c	R5	MRO_URE1 self-reported noncompliance with CIP-006-3c R5 for failing to monitor a physical access point of a designated Physical Security Perimeter (PSP). MRO_URE1's air conditioning unit located inside its Physical Security Perimeter (PSP) was not functioning, resulting in an elevation of temperature in this room. Inside the room lies communications equipment for MRO_URE1's communications network, used to connect and monitor field equipment to the primary control center. This room also houses the equipment associated with the operation of MRO_URE1's Energy Management System (EMS). Rising temperature in this room could cause failures with this equipment. To reduce the elevated heat in the room, Doors 4 and 5 of the PSP were propped open. Specifically, Door 4 was propped open for approximately one hour. Door 5 was propped open for approximately 14 hours. Door 4 leads into a hallway, while Door 5 leads into the Communications Department work area. The Communications Department work area has a door which leads into the same hallway as Door 4, and this door has a key lock on the door knob. There are no other doors that can provide access to the Communications Department work area besides Door 5 and the door leading into the hallway. While Door 4 was propped open, the operator on duty monitored the door for any unauthorized physical access to the PSP. While Door 5 was propped open, the Communications Department work area was locked down by locking the door that leads to the same hallway as Door 4. While Door 5 was propped open, there was no human observation of the access point.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Access to the building in which the rooms in question are located is controlled at all times. The incident occurred on a Sunday afternoon, continuing through Monday morning, so activity in the building was minimal. Additionally, physical access logs were reviewed. According to the logs, during the time that Door 4 was open, only one individual without authorized unescorted physical access was present in the building. In addition, the operator was present the entire time Door 4 was open. Because of the raised flooring in the area, the operator can hear if someone is present in the adjacent rooms. During the time that Door 5 was open, the door between the room and the adjacent hallway was locked and could only be opened/unlocked from the inside. It is only opened/unlocked during the day, when the room is manned. According to the logs, one of the individuals that works in the room was present for a portion of the duration of the issue. From that time onward, there was human observation of Door 5. No additional individuals without unescorted physical access entered the building prior to that time. Given the limited activity in the building, and the fact that PSP access was effectively controlled for the majority of the time because of Door 5 was locked, MRO determined that this issue posed a minimal risk to the BPS.	MRO_URE1 performed the following actions to mitigate the issue: 1) Discussed the physical security plan with supervisors and reminded them of the importance of security and raised awareness of the security restrictions for the PSP; 2) Trained staff on security awareness regarding propped open doors, presence of unauthorized individuals, and the risks associated with such situations; and 3) Included a quarterly article in the company newsletter to provide information on existing MRO_URE1 policy, or changes related to the NERC Reliability Standards, and general information related to NERC and cybersecurity.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010277	CIP-003-3	R5; R5.1	RFC_URE1 self-reported an issue with CIP-003-3 R5 to Reliability*First*. RFC_URE1 stores its Critical Cyber Asset (CCA) information in electronic files within a document management system and at specific locations at a generating plant. While RFC_URE1 verified the list of personnel responsible for authorizing access to CCA information within the document management system in 2011, RFC_URE1 failed to verify the list of personnel responsible for authorizing access to CCA information at the generating plant in 2011. RFC_URE1 documented and approved the two changes to the list of personnel responsible for authorizing access through its change management process.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). RFC_URE1's internal controls, specifically preparation for the annual CIP self-certification, enabled RFC_URE1 to discover and remediate the issues. In addition, RFC_URE1 documented and approved the two changes to the list of personnel responsible for authorizing access through RFC_URE1's change management process. The list of personnel responsible for authorizing access is six people, and the two individuals who approve such authorizing authority during this period were aware that the six individuals were responsible for authorizing access. As a result, it was less likely that anyone would have been improperly included on the list of personnel responsible for authorizing access to CCA information.	RFC_URE1 created and implemented a compliance action item tool to alert the appropriate personnel of specific compliance actions to be taken and the due date for each action. RFC_URE1 trained all necessary personnel on this tool.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010278	CIP-005-1	R2; R2.6	RFC_URE1 self-reported an issue with CIP-005-1 R2 to Reliability*First* . RFC_URE1 discovered that 16 of its firewalls, which are Cyber Assets that reside within an Electronic Security Perimeter, were displaying the appropriate use banner after the login process is completed rather than prior to login. RFC_URE1 failed to submit a Technical Feasibility Exception (TFE) for this issue.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The incorrect implementation of the appropriate use banner does not affect operation of the firewalls. In addition, the following compensating measures, as submitted in the TFE, have been in place for several years. RFC_URE1 physically stores all devices within a controlled access Physical Security Perimeter. RFC_URE1 also enables and monitors security logging for unauthorized access attempts, and configuration changes. Furthermore, an intrusion detection system actively monitors for anomalous traffic. Lastly, logon banners are correctly presented prior to login and are presented in a secure shell session after login and must be acknowledged before the session can continue.	RFC_URE1 completed the following mitigating actions: 1) employed the use of banners on three firewalls; 2) submitted a TFE for 12 firewalls; and 3) replaced one firewall with a model able to timely display the appropriate use banner.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010323	CIP-007-3	R2; R.2.1	RFC_URE1 self-reported an issue with CIP-007-1 R2 to Reliability*First* . Specifically, RFC_URE1 had not enabled only those ports and services required for normal and emergency operations. RFC_URE1 had disabled other ports and services on four printers and two time servers, the only function of which is to provide accurate time.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The printers at issue are not accessible from outside the RFC_URE1 system and are not connected to the Internet. In addition, the printers have directory service security groups established to limit unauthorized access to them. The time servers at issue are not connected to the Internet and have no visibility from the corporate or outside networks, though they do allow time synchronization with the local control system network. The only function of the time servers is to provide accurate time. RFC_URE1 installs, maintains, and monitors antivirus on the time servers appropriately. Furthermore, RFC_URE1 configured the Electronic Security Perimeter (ESP) to restrict access to these devices, enabled logging and monitored those logs for unauthorized access attempts and configuration changes. Lastly, an intrusion detection system actively monitors for anomalous traffic.	RFC_URE1 removed the printers from within the ESP and restricted the ports and services of the time servers.

Attachment A-2
December 31, 2012 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*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010324	CIP-007-1	R4	RFC_URE1 self-reported an issue with CIP-007-1 R4 to Reliability*First* . RFC_URE1 discovered that it had not installed antivirus software and malware prevention tools on 18 printers and two time servers because it is not technically feasible to do so. RFC_URE1 failed to submit a Technical Feasibility Exception (TFE) for these Cyber Assets, which are located within the Electronic Security Perimeters (ESPs).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The printers at issue are not accessible from outside the RFC_URE1 system and are not connected to the Internet. In addition, the printers have directory service security groups established to limit unauthorized access to them. Futhermore, the time servers at issue, although they do allow time synchronization with the local control system network, are not connected to the Internet and have no visibility from the corporate or outside networks. The only function of the time servers is to provide accurate time. Also, the following compensating measures, as submitted in the TFE, have been in place for several years: 1) appliances are physically stored in a controlled access physical security perimeter; 2) logical access is controlled by directory service group membership, remote authentication is controlled by directory service protocol authentication, and all authentications enforce password complexity; 3) security logging is enabled and monitored for unauthorized access attempts; 4) there is an intrusion detection system actively monitoring for anomalous network traffic; 5) local administrative passwords are set manually to meet (or exceed) the NERC CIP password complexity requirements; and 6) all servers and workstations based on a specific operating system have antivirus installed, maintained, and monitored appropriately.	RFC_URE1 replaced or installed a firmware upgrade to the time servers enabled installation of antivirus and malware prevention or submitted a TFE for those time servers where it was not possible to do so. In addition, RFC_URE1 removed certain printers from within the ESP and submitted a TFE for certain printers.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010325	CIP-007-1	R5; R5.3	RFC_URE1 self-reported an issue with CIP-007-1 R5 to Reliability*First*. RFC_URE1 discovered that it had not required passwords to have the following characteristics: 1) a minimum of six characters; 2) a combination of alpha, numeric and "special" characters; and 3) are changed at least annually on 18 printers and two time servers because it is not technically feasible to do so. RFC_URE1 failed to submit a Technical Feasibility Exception (TFE) for these Cyber Assets within the Electronic Security Perimeter (ESP).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The printers at issue are not accessible from outside the RFC_URE1 system and are not connected to the Internet. The time servers at issue, although they do allow time synchronization with the local control system network, are not connected to the Internet and have no visibility from the corporate or outside networks. The only function of the time servers is to provide accurate time. In addition, the following compensating measures for printers, as submitted in the TFE, have been in place for several years: 1) all printers are physically stored within a controlled access Physical Security Perimeter (PSP); 2) procedural controls are in place to manually enforce password requirements for: a) a six-character minimum length; b) a combination of alpha, numeric and special characters; and c) annual password reset; 3) remote logical access to printer interface is controlled by directory service authentication; 4) security logging is enabled and monitored for unauthorized access attempts; and 5) there is an intrusion detection system actively monitoring for anomalous traffic. For the servers, the following compensating measures, as submitted in the TFE, have been in place since 2012: 1) time server appliances are physically stored within an access controlled PSP; 2) access to these devices are controlled within the ESP; 3) only ports and services required for normal operation of the device are enabled; 4) logging is enabled and monitored for unauthorized access attempts and configuration changes; and 5) passwords for devices are under the control of three individuals who are aware of the password complexity requirements and of RFC_URE1's cybersecurity policy stating those requirements, therefore no password would be entered that did not meet the Standards.	RFC_URE1 replaced or installed a firmware upgrade to the time servers, enabled installation of antivirus and malware prevention or submitted a TFE for those time servers where it was not possible to do so. In addition, RFC_URE1 removed certain printers from within the ESP and submitted a TFE for certain printers.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010326	CIP-007-1	R6; R6.1	RFC_URE1 self-reported an issue with CIP-007-1 R6 to Reliability*First*. RFC_URE1 discovered that it had not ensured four printers and two time servers were implementing automated tools or organizational process controls to monitor system events that are related to cybersecurity because it is not technically feasible to do so. RFC_URE1 failed to submit a Technical Feasibility Exception (TFE) for these Cyber Assets within the Electronic Security Perimeter (ESP).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The printers at issue are not accessible from outside the RFC_URE1 system and are not connected to the Internet. In addition, the printers have directory service security groups established to limit unauthorized access to them. The time servers at issue, although they do allow time synchronization with the local control system network, are not connected to the Internet and have no visibility from the corporate or outside networks. The only function of the time servers is to provide accurate time. RFC_URE1 installs, maintains, and monitors antivirus on the time servers appropriately. Furthermore, RFC_URE1 configured the ESP to restrict access to these devices, enabled logging and monitored those logs for unauthorized access attempts and configuration changes. Lastly, an intrusion detection system actively monitors for anomalous traffic.	RFC_URE1 removed the printers from within the ESP and replaced or updated firmware for the time servers.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010327	CIP-007-3	R8; R8.2	RFC_URE1 self-reported an issue with CIP-007-3 R8 to Reliability*First* . RFC_URE1 discovered that it had not included in its cyber vulnerability assessment a review to verify that only ports and services required for operation of four printers and two time servers, Cyber Assets within the Electronic Security Perimeter (ESP), are enabled.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The printers at issue are not accessible from outside the RFC_URE1 system and are not connected to the Internet. In addition, the printers have directory service security groups established to limit unauthorized access to them. The time servers at issue, although they do allow time synchronization with the local control system network, are not connected to the Internet and have no visibility from the corporate or outside networks. The only function of the time servers is to provide accurate time. RFC_URE1 installs, maintains, and monitors antivirus on the time servers appropriately. Furthermore, RFC_URE1 configured the ESP to restrict access to these devices, enabled logging and monitored those logs for unauthorized access attempts and configuration changes. An intrusion detection system actively monitors for anomalous traffic.	RFC_URE1 removed the printers from within the ESP and restricted the ports and services of the time servers.

Attachment A-2

December 31, 2012 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*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010410	CIP-006-3c	R6	RFC_URE1 self-reported an issue with CIP-006-3c R6 to Reliability*First.* A RFC_URE1 employee without authorized unescorted physical access to a control room was working in that control room. A RFC_URE1 employee with authorized unescorted physical access to the control room escorted the unauthorized employee, but failed to manually log the unauthorized employee's access.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. RFC_URE1's internal controls enabled RFC_URE1 to discover and remediate the issues quickly. In addition, the employee was escorted at the time of the incident and was just not documented in the manual log. Furthermore, it was unlikely that the employee was a threat to RFC_URE1's system because the employee works for RFC_URE1 and RFC_URE1 had scheduled the employee to be in the control room that day.	RFC_URE1 restricted escorted visitor access to only one door, deactivated remote door unlock functionality of certain doors, and investigated other locations that have remote door unlock capabilities and evaluated them for deactivation.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201100537	CIP-007-3	R4	SPP RE_URE1 self-reported noncompliance with CIP-007-3 R4, regarding its failure to install malware prevention software on its Critical Cyber Assets (CCA). SPP RE_URE1 filed a Technical Feasibility Exception for its Cyber Assets using its operating system because these assets were not running anti-virus and malware protection software, and SPP RE_URE1 had been instructed by its supervisory control and data acquisition (SCADA) vendor that anti-virus and malware protection programs had not been approved or tested for these assets. This TFE was accepted by SPP RE. SPP RE disapproved the TFE because it determined that anti-virus products were available for the operating system. The TFE disapproval was made effective March 1, 2011. SPP RE_URE1 self-reported a noncompliance of CIP-007-3 R4 because it failed to install and began running anti-virus software on its operating system Cyber Assets until 22 days after the TFE disapproval effective date.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1 allowed 22 days to pass between the effective disapproval date and the date in which it installed and began running anti-virus software on its operating system Cyber Assets, SPP RE_URE1's Cyber Assets were still under the protective mitigation measures that it had implemented for the TFE. These protective measures included housing all assets behind a firewall, which was set to deny access by default, and monitoring these assets 24 hours a day, seven days a week by a security event and incident management server, which is set to alert administrators of suspicious activities. Additionally, SPP RE_URE1's Cyber Assets that used the operating system had patches applied, and these patches were kept up to date. Therefore, although these devices did not have anti-virus or malware prevention tools, they were protected from vulnerabilities.	SPP RE_URE1 implemented anti-virus software on operating systems and enrolled these systems in SPP RE_URE1's CIP-007 R4 Anti-malware and Anti-virus Program.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201210282	CIP-005-1	R1; R1.6	During a Compliance Audit, the SPP RE Audit Team determined that SPP RE_URE2 was noncompliant with CIP-005-1 R1 and R1.6. With regard to CIP-005-1 R1, the Audit Team found that SPP RE_URE2's documentation of its Electronic Security Perimeter (ESP) did not properly identify five firewalls that existed beyond the ESP. The firewalls' management ports were connected to a network segment within the ESP. Additionally, SPP RE_URE2 had not appropriately identified three host servers which were serving as access control devices between the GPS clocks and the SPP RE_URE2 system control and data acquisition (SCADA)/energy management systems (EMS) as Electronic Access Control Systems (EACS) /ESP access points. With regard to R1.6, the Audit Team found that SPP RE_URE2's documentation supporting compliance with CIP-005-1 R1.6, i.e., the lists of Critical Cyber Assets (CCAs), Protected Cyber Assets, Electronic Access Control and monitoring Systems, and Physical Access Control Systems (collectively Master Lists) did not properly identify the active directory servers, the firewall management console, and the firewall as EACS.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE2 did not properly identify all electronic access points to the ESPs and the Cyber Assets deployed for the access control and monitoring of these access points on its master lists, SPP RE_URE2 did have the controls required by CIP-005-1 R1.5 in place prior to October 1, 2010. Therefore, all affected Cyber Assets and CCAs were afforded protective measures in accordance with the CIP Standards. SPP RE_URE2's non-compliance was documentation-related and did not represent a material lapse in the protection of its ESPs, CCAs or Cyber Assets deployed for the access control and monitoring of its access points.	SPP RE_URE2 modifed its master lists as follows: 1) reclassified the five firewalls beyond the defined ESP, whose management ports are connected to a network segment within the ESP; 2) identified and classified three host servers serving as the access point control devices between the GPS clocks and the SCADA/EMS servers as EACS / ESP Access Points on the master lists; 3) updated its ESP diagrams to more clearly designate all ESP access points; and 4) added two active directory servers to the master lists as EACS for their access control and monitoring functions. The administrative error that temporarily omitted the firewall management console from the master lists was corrected. SPP RE_URE2 reviewed the versions of the master lists and validated that the firewall and the firewall management console were correctly listed.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201210284	CIP-005-1	R3	During a Compliance Audit, the SPP RE Audit Team determined that SPP RE_URE2 was noncompliant with CIP-005-1 R3. SPP RE_URE2 was not performing monitoring and logging of access attempts at all of the access point to its Electronic Security Perimeters (ESPs) twenty-four hours a day, seven days a week. SPP RE_URE2 had implemented a process for monitoring and logging access at access points to its ESP which relied on its ConsoleWorks server to monitor and automatically review logs for Virtual Private Network (VPN) access and access to the Cyber Assets within its ESPs. ConsoleWorks provides real-time alerts of failed logon attempts. The Audit Team found that SPP RE_URE2 was not capturing and manually reviewing all access logs when the ConsoleWorks server is down for maintenance.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The SPP RE Audit Team determined that SPP RE_URE2 had implemented and documented processes for monitoring and logging access at access points to its ESPs twenty-four hours a day, seven days a week. It was only during those brief periods when the ConsoleWorks server was down for maintenance that logs for VPN access and access to the Cyber Assets in SPP RE_URE2's ESPs were not captured and automatically reviewed. Electronic dial-up access to SPP RE_URE2's ESPs and Cyber Assets is not allowed and access to firewalls is monitored through a separate process in which firewall logs are monitored and alerts are sent to SPP RE_URE2 IT Security Staff on failed access attempts. SPP RE_URE2 maintains a robust physical security program providing in-depth protection to its Cyber Assets.	SPP RE_URE2 implemented a second ConsoleWorks server to provide for continuous monitoring and automatic reviews of logs for VPN access and access to the Cyber Assets in its ESP when one of its ConsoleWorks servers is offline for maintenance.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201210285	CIP-006-3	R1; R1.6	During a Compliance Audit, the SPP RE Audit Team determined that SPP RE_URE2 was noncompliant with CIP-006-3 R1.6. SPP RE_URE2's manual visitor log for the Physical Security Perimeter (PSP) at SPP RE_URE2's central control center did not denote the exit time for one visitor.	The SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The SPP RE Audit Team determined that SPP RE_URE2 had implemented procedures at each of its PSPs to manually or electronically log access information details that are sufficient to uniquely identify individuals not authorized for unescorted access, and to identify the date and time of access of these individuals. SPP RE_URE2's physical access program was sufficiently robust to provide substantial protection to its PSPs. The issue represented a single lapse in SPP RE_URE2's physical security program and is not indicative of a systemic problem.	SPP RE_URE2 verified that its physical security plan and corresponding visitor control program contained the necessary language pertaining to the requirement to log the entry and exit of visitors to restricted areas, including the date and time, to and from PSPs. It validated that the log controllers and security services are reviewing restricted area visitor logs to ensure required information is documented and legible. SPP RE_URE2 added an additional camera installation on the inside of the PSP Access Point to record the logging of visitors to supplement the requirement to log visitor access to restricted areas.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201210288	CIP-007-1	R6;	During a Compliance Audit, the SPP RE Audit Team determined that SPP RE_URE2 was noncompliant with CIP-007-1 R6. SPP RE_URE2 had not properly implemented automated tools or organizational process controls to monitor system events that are related to cyber security. SPP RE_URE2 had implemented a process for monitoring and logging access at access points to its Electronic Security Perimeter (ESP) which relied on the ConsoleWorks server to monitor system events, send alerts and automatically review logs for Virtual Private Network (VPN) access and access to the Cyber Assets in its ESPs. The Audit Team found that SPP RE_URE2 was not receiving alerts of detected cyber security incidents nor capturing and manually reviewing all logs of system events related to cyber security when the ConsoleWorks server is down for maintenance.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The SPP RE Audit Team determined that SPP RE_URE2 had implemented and documented processes for monitoring and logging access at access points to its ESPs twenty-four hours a day, seven days a week. These processes provided SPP RE_URE2 with alerts of detected cyber security incidents and ensured that logs of system events related to cyber security were captured. It was only during those brief periods when the ConsoleWorks server was down for maintenance that alerts were unavailable and logs for VPN access and access to the Cyber Assets in its ESPs were not captured and automatically reviewed. Additionally, SPP RE_URE2 had protective measures in place to protect Cyber Assets and Critical Cyber Assets during the isolated times the ConsoleWorks server was down for maintenance, including card swipes for sensitive areas, locking drawers, video surveillance, password and lockout policies, and personnel physical and cyber access reviews and control processes.	SPP RE_URE2 installed a second server running ConsoleWorks as a backup. Security event logs are sent to both the primary and backup ConsoleWorks servers to evaluate, capture, and alert. Automated failover is configured, as is the ability to manually switch for routine maintenance activities. The ConsoleWorks server was reconfigured to store security event logs indefinitely.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP RE_URE3)	NCRXXXXX	SPP2012009933	CIP-007-3	R1.3	During a CIP Compliance Audit, the SPP RE CIP Audit Team determined that SPP RE_URE3 was noncompliant with CIP-007-3 R1. SPP RE_URE3 did not have documentation of test results for changes to Cyber Assets (CAs) within the Electronic Security Perimeter (ESP) as required by R1.3. The SPP Audit Team discovered the noncompliance while reviewing SPP RE_URE3's test procedures for adding new CAs to the ESP or significantly changing existing CAs within the ESP.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE3 did not have documentation of the test results for new CAs or changes to existing CAs, the CIP Audit Team found that SPP RE_URE3 had change management tickets directing the testing of changes to CAs within the ESP. SPP RE_URE3's change management records included observation comments for changes made to SPP RE_URE3 CAs within the ESP. While these comments do not constitute test results, they do evidence that changes took place under SPP RE_URE3 observation.	SPP RE_URE3 has incorporated a description of the test it performed on any changes to CAs within the ESP as well as the results of those tests into its change management tickets.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE2012011001	CIP-003-3	R2; R2.1; R2.2	Texas RE_URE1 submitted a Self-Report after an internal audit revealed that the change in senior managers with overall responsibility and authority for leading and managing Texas RE_URE1's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3 was not documented within 30 days, as required by CIP-003-3 R2.2. The operation supervisor served as a senior manager for two years and one month and this designation was documented pursuant to CIP-003-1 R1 criteria. However, when the operation supervisor left, the appointment of the new senior manager was not documented to reflect the change. In addition, Texas RE_URE1 self-reported that it failed to show documentation of how the new senior manager hired was identified in Texas RE_URE1's documents by name, title, and date of designation, as required by CIP-003-3 R2.1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). Although Texas RE_URE1 failed to document the designation of the new senior manager within 30 days, the senior manager was operating in his new capacity and was clear about his overall responsibility and authority for leading and managing Texas RE_URE1's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3. Further, due to the small staff size, Texas RE_URE1 reported that all the employees were made aware verbally of the new senior manager and his role within the company. Finally, Texas RE_URE1 did not experience a gap in senior leadership for CIP Standards, thereby reducing the risk to the BPS to minimal.	This remediated issue was mitigated when the leadership delegation document, identifying the senior manager, was signed. Texas RE has verified the mitigation activities as complete. To prevent future oversights and to ensure timely replacement of departing senior managers, a transfer note with instructions were placed in the personnel file of the person who is presently designated as the senior manager. The note clarifies that: 1) he is the senior manager for the applicable CIP Standards; and (2) he must take appropriate action to properly transfer the senior manager duties and responsibilities prior to his departure, retirement or other personnel status change. Also, Texas RE_URE1 has adopted and implemented a CIP document that specifically states that changes to the senior manager position must be documented within 30 days of the change.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE2012010376	CIP-002-3	R1	An Audit conducted by Texas RE revealed that Texas RE_URE2 failed to identify and document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. A draft RBAM document existed since mid-March, 2012, but it was not approved and had not been implemented. An approved RBAM was submitted to the Audit Team. Texas RE determined the duration of this remediated issue to be five weeks, from the date when Texas RE_URE2 was required to comply with this Standards, to the date when the RBAM was approved and documented.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Texas RE_URE2 does not have any Critical Assets or Critical Cyber Assets (CCAs). In addition, Texas RE_URE2 provided RBAM, showing that Texas RE_URE2 went through the Critical Asset criteria included in the approved RBAM and found no Critical Assets or CCAs, indicating that during the pendency of this remediated issue, Texas RE_URE2 had no Critical Assets or CCAs. Further, Texas RE_URE2's Transmission Operator provided documentation indicating that it did not consider Texas RE_URE2's assets to be critical. Finally, the period of noncompliance was five weeks, thereby reducing the risk to the BPS.	Texas RE_URE2 took immediate action to correct this remediated issue. The senior manager with overall responsibility and authority for leading and managing Texas RE_URE2's implementation of, and adherence to all CIP Standards approved and implemented an RBAM. Texas RE_URE2 provided Texas RE with an approved, implemented, and completed RBAM and a list of Critical Assets and CCAs, which showed that Texas RE_URE2 did not have any Critical Assets or CCAs. Texas RE has verified the mitigation activities as complete.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE2012010377	CIP-002-3	R3	An Audit conducted by Texas RE revealed that Texas RE_URE2 failed to develop a list of associated Critical Cyber Assets (CCAs) essential to the operation of its Critical Assets. During the period of noncompliance, Texas RE_URE2 did not have a documented RBAM, and therefore could not identify a list of Critical Assets through application of its RBAM. However, Texas RE_URE2 had a draft RBAM during that period. Because Texas RE_URE2 did not have a list of Critical Assets, it could not develop a list of associated CCAs. Texas RE determined the duration of this remediated issue to be five weeks, from the date when Texas RE_URE2 was required to comply with this Standards, to the date when the RBAM was approved and documented and Texas RE_URE2 developed a list of Critical Assets and associated CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Texas RE_URE2 does not have any Critical Assets or CCAs. Texas RE_URE2 provided a list of assets through the risk assessment criteria included in the approved RBAM. The list showed that Texas RE_URE2 has no Critical Assets or CCAs. Additionally, Texas RE_URE2's Transmission Operator provided documentation indicating that it did not consider Texas RE_URE2's assets to be critical. Finally, the period of noncompliance was five weeks, thereby reducing the risk to the BPS.	Texas RE_URE2 took immediate action to correct this remediated issue. The senior manager with overall responsibility and authority for leading and managing Texas RE_URE2's implementation of, and adherence to all CIP Standards accepted and implemented an RBAM. Texas RE_URE2 provided Texas RE with an approved, implemented, and completed RBAM and a list of Critical Assets and CCAs, which showed that Texas RE_URE2 did not have any Critical Assets or CCAs. Texas RE has verified the mitigation activities as complete.

- Optim Energy Altura Cogen, LLC (Optim)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE2012010378	CIP-002-3	R4	An Audit conducted by Texas RE revealed that Texas RE_URE2 was noncompliant with CIP-002-3 R4. Texas RE_URE2's senior manager or delegate(s) failed to approve annually the risk-based assessment methodology (RBAM), the list of Critical Assets and the list of Critical Cyber Assets (CCAs). Texas RE verified that the entity documented and implemented a RBAM. Texas RE determined the duration of this remediated issue to be five weeks, from the date when Texas RE_URE2 was required to comply with this Standards, to the date when the senior manager approved the RBAM and the list of CA and CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). While the RBAM and the list of Critical Assets and CCAs were not formally accepted and signed by the senior manager, an evaluation of the assets was performed using the implemented RBAM and no Critical Assets or associated CCAs were found Additionally, Texas RE_URE2's Transmission Operator provided documentation indicating that it did not consider Texas RE_URE2's assets to be critical. Finally, the period of noncompliance was five weeks, thereby reducing the risk to the BPS.	Texas RE_URE2 took immediate actions to correct this remediated issue. The senior manager with overall responsibility and authority for leading and managing Texas RE_URE2's implementation of and adherence to all CIP standards accepted and implemented an RBAM. Texas RE_URE2 provided Texas RE with an approved, implemented, and completed RBAM and a list of Critical Assets and CCAs. Texas RE has verified the mitigation activities as complete.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE2012010379	CIP-002-3	R2	An Audit conducted by Texas RE revealed that Texas RE_URE2, failed to develop a list of its identified Critical Assets determined through an annual application of its risk-based assessment methodology (RBAM), as required by CIP-002-3 R2. During the period of noncompliance, Texas RE_URE2 did not have a documented and approved RBAM, and therefore could not identify a list of Critical Assets through the application of its RBAM. However, Texas RE_URE2 had a draft RBAM during this period. Texas RE determined the duration of this remediated issue to be five weeks, from the date when Texas RE_URE2 was required to comply with this Standards, to the date when the RBAM was approved and documented and Texas RE_URE2 developed a list 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 (BPS) because Texas RE_URE2 does not have any Critical Assets or Critical Cyber Assets (CCAs). Texas RE_URE2 provided a list of assets evaluated through the risk assessment criteria included in the approved RBAM. The list showed that Texas RE_URE2 has no Critical Assets or CCAs. Additionally, Texas RE_URE2's Transmission Operator provided documentation indicating that it did not consider Texas RE_URE2's assets to be critical. Finally, the period of noncompliance was five weeks, thereby reducing the risk to the BPS.	Texas RE_URE2 took immediate action to correct this remediated issue. The senior manager with overall responsibility and authority for leading and managing Texas RE_URE2's implementation of, and adherence to all CIP Standards accepted and implemented an RBAM. Texas RE_URE2 provided Texas RE with an approved, implemented, and completed RBAM and a list of Critical Assets and CCAs, which showed that Texas RE_URE2 did not have any Critical Assets or CCAs. Texas RE has verified the mitigation activities as complete.

Document Accession #: 20121231-5257 **Filed Date: 12/31/2012**

Document Content(s)