Federal Energy Regulatory Commission
Washington, D.C. 20426

December 29, 2021

Release Letter and Determination
Letter re: RC13-10
FOIA No. FY19-30

VIA EMAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated December 15, 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. RC13-10, along with the names of eight (8) relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC13-10

With respect to the remaining identities of UREs contained in RC13-10, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the

[1] 5 U.S.C. § 552 (2018).

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

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC13-10 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: 2021.12.29 15:29:23 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

June 27, 2013

RC13-10

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

Univer

Southern Minnesota Municipal Power Agency (SMMPA)-.pdf page 30
City Of Grand Island, NE (GRIS)-.pdf page 30
Dearborn Industrial Generation, L.L.C. (Dearborn)-.pdf page 32
LSP University Park, LLC (LSP University Park) - .pdf page 35
PPG Industries, Inc. (PPG - .pdf page 35
Barney M Davis Unit 1 (BMD1) - .pdf page 36
Barney M Davis LP (BMDLP) - .pdf page 36
Grand Coulee Project Hydroelectric Authority (GCPH)- .pdf page 37

Re: NERC FFT Informational Filing
FERC Docket No. RC13-_

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 52 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 93 possible violations[5] of 22 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

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

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

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.

Statement Describing the Resolution[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the

[6] *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) ("March 15, 2012 CEI Order"); *see also North American Electric Reliability Standards Development and NERC and Regional Entity Enforcement*, 132 FERC ¶ 61,217 at P.218 (2010)(encouraging streamlined administrative processes aligned with the significance of the subject violations).
[7] *See* 18 C.F.R § 39.7(d)(7).
[8] *See* 18 C.F.R § 39.7(d)(4).

August 27, 2010 Guidance Order,[9] NERC Enforcement staff under delegated authority from the NERC BOTCC, approved the FFT based upon its findings and determinations, as well as its review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the remediated issues.

Notice of Completion of Enforcement Action

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

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

Request for Confidential Treatment of Certain Attachments

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

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

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

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

Attachments to be included as Part of this FFT Informational Filing

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

a) FFT Spreadsheet, included as Attachment A; and

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

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Sonia C. Mendonca* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 edwin.kichline@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Sonia C. Mendonca

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

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

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

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

cc: Entities listed in Attachment B

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

FOR FRCC:

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

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

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

For MRO:

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

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

FOR 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

Niki Schaefer*
Managing Enforcement Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
Niki.schaefer@rfirst.org

FOR SERC:

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

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

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

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

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

FOR SPP RE:

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

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

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

FOR TEXAS RE:

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

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

FOR WECC:

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

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

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

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

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
June 27, 2013

Take notice that on June 27, 2013, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding fifty-two (52) Registered Entities in seven (7) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Attachment A-1

June 27, 2013 Public Non-CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet (Non-CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council (FRCC)	New Smyrna Beach, Utilities Commission of (NSB)	NCR00052	FRCC2012010053	BAL-001-0	R1	On April 6, 2012, NSB submitted a Self-Report stating that, as a Balancing Authority, it had an issue with BAL-001-0 R1. NSB could not demonstrate that it had operated such that the average of the clock-minute averages (using Area Control Error (ACE)) was less than the limit allowed in the Standard. NSB stated that it had depended upon its services provider to: 1) include NSB within the service provider's own calculation of Control Performance Standards (CPS1) 1; and 2) ensure that NSB's ACE operated within limits required by the Standard. NSB, however, became aware that the contract with its service provider did not include overlapping service and thus NSB's CPS1 was not being calculated separately.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NSB was using a long-term interchange contract for supplemental regulation and was supplying its ACE to the entity, Progress Energy Florida, performing that service. NSB's ACE was included in its regulation service provider's so reliability was not impacted. Furthermore, NSB is a very small utility that has non-regulated generation and only 11 miles of BPS transmission line (less than 1% of Regional transmission line) with an all time peak load of 109 MW.	To mitigate this issue, NSB upgraded its supervisory control and data acquisition system with a scheduled change which included a module to automatically calculate CPS 1 and 2 values and meet performance criteria on its own. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	New Smyrna Beach, Utilities Commission of (NSB)	NCR00052	FRCC2012010054	BAL-001-0	R2	On April 6, 2012, NSB submitted a Self-Report stating that, as a Balancing Authority, it had an issue with BAL-001-0 R2. NSB could not demonstrate that it had operated such that its average Area Control Error (ACE) for at least 90% of clock-ten-minute periods during a calendar month was within the limit allowed in the Standard. NSB stated that it had depended upon its services provider to: 1) include NSB within the service provider's own calculation of Control Performance Standards 2 (CPS2); and 2) ensure that NSB's ACE operated within limits required by the Standard. NSB, however, became aware that the contract with its service provider did not include overlapping service and thus NSB's CPS2 was not being calculated separately.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NSB was using a long-term interchange contract for supplemental regulation and was supplying its ACE to the entity, Progress Energy Florida, performing that service. NSB's ACE was included in its regulation service provider's so reliability was not impacted. Furthermore, NSB is a very small utility that has non-regulated generation and only 11 miles of BPS transmission line (less than 1% of Regional transmission line) with an all time peak load of 109 MW.	To mitigate this issue, NSB upgraded its supervisory control and data acquisition system with a scheduled change which included a module to automatically calculate CPS 1 and 2 values and meet performance criteria on its own. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Orlando Utilities Commission (OUC)	NCR00057	FRCC2012009679	VAR-001-1	R6	On January 31, 2012, NSB submitted a Self-Report that, as a Transmission Operator, it had an issue with VAR-001-1 R6. NSB did not know the status of all transmission Reactive Power resources, including the status of voltage regulators.	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 voltage regulator was not set in a manual mode but rather was set to automatic in MVAR control, and the actual mode of control for the unit's regulator did provide a level of voltage stability to the BPS.	To mitigate this issue, OUC: 1) implemented a process with procedure and training to verbally verify and record status; 2) implemented unit excitation status telemetry; and 3) developed coordination procedure and training. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Orlando Utilities Commission (OUC)	NCR00057	FRCC2012009954	FAC-009-1	R1	On March 23, 2012, FRCC conducted a Compliance Audit of NSB and determined that NSB, as a Generator Owner, had an issue with FAC-009-1 R1. NSB did not have sufficient evidence to demonstrate it had established Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings methodology. Specifically, Indian River Plant (IRP) Combustion Turbine (CT)-C, CT-D, and Stanton Energy Center Combined Cycle (SEC) B had determined a most limiting piece of equipment for those facilities. In both cases, however all component ratings from the methodology were not evaluated and therefore the most limiting piece of equipment could not be substantiated.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. OUC was operating to manufacturer's ratings, had proven operational history with no actual impact based on the established ratings, and once the complete ratings were established there was no change in the most limiting piece of equipment.	To mitigate this issue, OUC: 1) updated their facility ratings analysis documents for the units IRP CT C and IRP CT D based on vendor responses to clearly identify the missing component ratings; 2) updated their facility ratings analysis document for the SEC CC B based on vendor documentation and engineering analysis. The engineering analysis established the overall Facility Ratings and documented any acceptance of loss-of-life on any component which would otherwise limit the output of the unit or limit the unit output; 3) identified the missing ratings for all the IRP units (with no change in rating after the review of most limiting factors); and 4) substantiated the existing generator rating associated with SEC unit B as being the most limiting since the generator output is constrained by the Combustion Turbine output capability. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Orlando Utilities Commission (OUC)	NCR00057	FRCC2012009955	MOD-001-1a	R2; R2.2; R2.3	On March 23, 2012, FRCC conducted a Compliance Audit of OUC and determined that OUC, as a Transmission Service Provider, had an issue with MOD-001-1a R2. In calculating firm Available Transfer Capability (ATC), OUC did not subtract Transmission Reliability Margin (TRM) from Total Transfer Capability (TTC) as described in its Area Interchange Methodology (MOD-028-1). Specifically, no TRM was subtracted for days two through seven (R2.2 and 2.3), no TRM was subtracted from the sum of the facility ratings segment (R2), and no TRM was calculated after April 30, 2012 (resulting in no TRM being calculated for at least the next 12 months) (R2.3).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. OUC had three import and three export paths, and there were no wheeling paths through OUC. In addition, when making a reservation it would need to be made through both the sending and receiving Transmission Service Providers (TSPs) on the path. Even though OUC was not correctly calculating firm ATC (by not subtracting TRM), the other TSP in the path should have been calculating firm ATC correctly by subtracting TRM and in any case that OUC would have tried to oversell firm ATC, the reservation would have been denied by the partner TSP. Furthermore, the sum of the facility (line) ratings are typically larger than the calculated TTC value and would not be a limiting factor even if TRM is not subtracted correctly.	To mitigate this issue, OUC: 1) began a solution identification; 2) had further discussion at Florida Transmission Capability Determination Group to draft TRM language to handle the static versus engine segment TRM; 3) issued a revised TRM implementation document (ID); 4) started utilizing the TRM_Adder_Hourly calculation function; 5) increased the end date on the TRM entries such that they were more than 26 months into the future so that values were available through the full horizon of calculations; and 6) reviewed and corrected any issues identified; modified TRM ID to correctly reflect the way TRM is calculated. Specifically, this is documenting the changes from a static TRM calculation to TRM that remains constant and then has a gradual reduction. FRCC has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council (FRCC)	Orlando Utilities Commission (OUC)	NCR00057	FRCC2012009956	MOD-001-1a	R3; R3.1	On March 23, 2012, FRCC conducted a Compliance Audit of OUC and determined that, as a Transmission Service Provider, OUC had an issue with MOD-001-1a R3. OUC failed to keep current its Available Transfer Capability Implementation Document (ATCID) to include the following information: a description of how the selected methodology has been implemented in such detail that, given the same information used by the Transmission Service Provider (TSP), the results of the Available Transfer Capability (ATC) calculations can be validated.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. OUC had three import and three export paths. There were no wheeling paths through OUC. In addition, when making a reservation, the reservation would need to be made through both the sending and receiving TSPs on the path. Even though OUC was not correctly calculating firm ATC (by not subtracting TRM), the other TSP in the path should have been calculating firm ATC correctly by subtracting TRM and in the case that OUC would have tried to oversell firm ATC, the reservation would have been denied by the partner TSP. In addition, the sum of the facility (line) ratings are typically larger than the calculated TTC value and would not be a limiting factor even if TRM is not subtracted correctly.	To mitigate this issue, OUC: 1) began a solution identification; 2) had further discussion at Florida Transmission Capability Determination Group to draft TRM language to handle the static versus engine segment TRM; 3) issued a revised TRM implementation document (ID); 4) started utilizing the TRM_Adder_Hourly calculation function; 5) increased the end date on the TRM entries such that they were more than 26 months into the future so that values were available through the full horizon of calculations; and 6) reviewed and corrected any issues identified; modified TRM ID to correctly reflect the way TRM is calculated. Specifically, this is documenting the changes from a static TRM calculation to TRM that remains constant and then has a gradual reduction. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Orlando Utilities Commission (OUC)	NCR00057	FRCC2012009957	MOD-008-1	R1; R1.3.2; R1.3.3	On March 23, 2012, FRCC conducted a Compliance Audit of OUC and determined that, as a Transmission Service Provider, it had an issue with MOD-008-1 R1. OUC had prepared but did not keep current its Transmission Reliability Margin (TRM) Implementation Document as required by the Standard. Specifically, the document states that OUC will subtract TRM from Total Transfer Capability (TTC) to calculate firm Available Transfer Capability (ATC), which had not been done. For R1.3.2 and R1.3.3, OUC did not actually document the process that had been implemented as no TRM was subtracted for days two through seven, no TRM was subtracted from the sum of the facility ratings segment, and no TRM was applied after April 30, 2012.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. OUC had three import and three export paths. There were no wheeling paths through OUC. In addition, when making a reservation, the reservation would need to be made through both the sending and receiving TSPs on the path. Even though OUC was not correctly calculating firm ATC (by not subtracting TRM), the other TSP in the path should have been calculating firm ATC correctly by subtracting TRM and in the case that OUC would have tried to oversell firm ATC, the reservation would have been denied by the partner TSP. In addition the sum of the facility (line) ratings are typically larger than the calculated TTC value and would not be a limiting factor even if TRM is not subtracted correctly.	To mitigate this issue, OUC: 1) began solution identification; 2) had further discussion at Florida Transmission Capability Determination Group to draft TRM language to handle the static versus engine segment TRM; 3) started utilizing the TRM_Adder_Hourly calculation function; 4) increased the end date on the TRM entries such that they were more than 26 months into the future so that values were available through the full horizon of calculations; and 5) modified the TRM ID document to correctly reflect the way TRM is calculated. Specifically this is documenting the changes from a static TRM calculation to TRM that remains constant and then has a gradual reduction. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Progress Energy Florida (PEF)	NCR00063	FRCC2013012470	EOP-005-1	R2	On June 7, 2013, FRCC conducted a Compliance Audit of PEF and determined that PEF as a Transmission Operator had an issue with EOP-005-1 R2. PEF failed to update its restoration plan when it made a change to its power system network. Specifically, PEF had a change in a loop section of its sample restoration plan provided to the system operators. This change was due to the removal of a 115 kV line. The 115 kV line was retired on December 17, 2012 and PEF removed the line from the one-line of the Energy Management System (EMS). The line was fully removed from the EMS on February 20, 2013. The restoration plan was corrected on June 5, 2013.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). This was a documentation issue. PEF performed simulations on January 31, 2013 and April 8, 2013 and the flexibility of the restoration plan allows for the closing of alternate lines, therefore the unavailability of this 115 kV line during multiple simulations had no impact in the restoration of the system.	To mitigate this issue, PEF: 1) immediately updated its restoration plan when it was discovered that there was an discrepancy in the restoration plan; and 2) placed subject matter experts (SMEs) for EOP-005 on the mailing list of the Equipment Status Report. This gives the SMEs notification of changes on the PEF power system network prior to the changes being implemented. The Equipment Status Report is an FRCC document that shows planned changes to the BPS in the FRCC region. FRCC has verified the completion of all mitigation activity.
Midwest Reliability Organization (MRO)	High Prairie Wind Farm II, LLC (HPWF)	NCR10161	MRO2012009682	PRC-005-1	R2; R2.1	During a Compliance Audit conducted between November 15, 2011 and November 17, 2011, MRO discovered that HPWF, as a Generator Operator and Generator Owner, failed to provide maintenance and testing evidence for one of its Protection System station batteries in accordance with the intervals defined in its Protection System maintenance and testing program, as required by PRC-005-1 R2.1. Specifically, HPWF failed to perform annual station battery testing in 2008. HPWF's generating plant began commercial operation in November 2007. Although HPWF performed a monthly test in November 2007 and December 2007 and a quarterly test in 2009, those tests were only a subset of the required annual test. HPWF's Protection System maintenance and testing program requires an annual test, not a monthly or quarterly test. Although HPWF was required to complete the annual test on or before November 2008, it did not perform the full annual test again until September 2009. Therefore, HPWF missed its annual maintenance and testing interval by nine months. MRO requested that HPWF perform a comprehensive review of its Protection System maintenance and testing records. HPWF reported that it has 9 relays, 5 voltage and current sensing devices, 2 station batteries, and 9 DC control circuits subject to PRC-005-1 R2. Of those devices, HPWF failed to provide maintenance and testing records for one station battery, or 4% of its devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). HPWF missed maintenance and testing for one station battery at one substation for one testing interval by approximately nine months. The plant began commercial operation in November 2007, and HPWF missed the maintenance and testing interval in November 2008. Therefore, the station battery was one year old when it missed its required interval. The facility consists of total installed capacity of 100.65 MW, provided by 61 1.65 MW turbines. Based on the duration of the issue, the other battery testing HPWF performed on a monthly and quarterly basis, the age of the station battery, and the size of HPWF, MRO determined that this issue posed a minimal risk to the BPS.	To mitigate the issue, HPWF: 1) performed the annual battery test on September 15, 2009; 2) implemented a more comprehensive battery testing procedure, to include additional monthly battery inspections in addition to annual battery testing; and 3) developed an internal process to integrate the management of all of its facility testing and maintenance processes and procedures. MRO has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Muscatine Power & Water (Board Of Water, Electric & Communications) (MPW)	NCR00967	MRO2013012071	PRC-005-1b	R2	On February 28, 2013, MPW submitted a Self-Report to MRO stating that, as a Transmission Owner and Distribution Provider, it had an issue with PRC-005-1b R2.1. MPW failed to provide evidence that the station battery tied to the Protection System devices was maintained and tested within the defined intervals pursuant to the Reliability Standard. Under MPW's Protection System maintenance and testing program, MPW is required to perform a capacity test on the station battery at its unit 9 161 kV substation within six-year intervals. MPW's capacity test was completed on July 19, 2006, which required MPW to complete its next capacity test by July 19, 2012. However, that test was completed on February 19, 2013, which was 217 days past due. MPW received an Administrative Citation for MRO201000194, a previous violation of PRC-005-1 R2, which was filed with FERC under NP11-133-000 on February 28, 2011. On March 25, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. In mitigating the previous violation, MPW provided in-house compliance training to substation personnel and completed an inventory of all Protection System components for the unit 9 161 kV substation, but failed to add an automatic notification for capacity testing. As a result, MPW missed the scheduled capacity testing by 217 days. MRO determined that the instant issue is appropriate for FFT treatment because it posed a minimal risk to the BPS based on the facts and that there are no other issues.	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 affected station battery comprised less than one percent of MPW's Protection System elements and the six-year testing interval was missed by seven months. In addition, MPW is a small entity located in Muscatine, Iowa with limited possible impact on the BPS. MPW serves approximately 11,300 electric customers owns and operates one BPS generator and 33 miles of 161 kV transmission line. The violation relates to only batteries at one transmission substation. Further, in addition to capacity testing every six years, MPW performs more frequent tests relating to the substation and battery to ensure proper performance. Lastly, the unit 9 161 kV substation batteries are monitored by MPW's supervisory control and data acquisition system, which provides continuous monitoring of the battery charger, DC system ground conditions, and the DC station service voltage.	To mitigate this issue, MPW: 1) performed the capacity test; 2) performed a comprehensive review of all MPW elements (both generation and transmission), subject to PRC-005-1b R2, to verify the maintenance activities described in the MPW Protection System maintenance and testing program have been performed within the required intervals; 3) created a work order entered into MPW's computerized maintenance management system (CHAMPS) on a six-year interval to create a purchase order for a capacity test; 4) created an auto-generated daily email from CHAMPS that lists all maintenance and testing activities on all MPW elements subject to PRC-005 and PRC-008 within 30 days of its due date for the managers of Reliability Standards compliance and transmission and distribution; 5) created a monthly reminder in Lotus Notes for the manager of Reliability Standards compliance to perform a monthly check of PRC-005 test records to verify that the PRC-005 maintenance activities are on schedule and added the capacity test task to the list; and 6) entered all maintenance work orders and station batteries subject to PRC-005-1b R2, into CHAMPS. MRO verified the completion of all mitigation activity on April 11, 2013.
Reliability*First* Corporation (Reliability*First)*	Commonwealth Edison Company (ComEd)	NCR08013	RFC2012010778	PRC-005-1a	R2; R2.1	On June 30, 2012, ComEd submitted a Self-Report to Reliability*First* stating that, as a Distribution Provider, it had an issue with PRC-005-1a R2.1. During the review of a daily preventative maintenance look-ahead report, ComEd found that Protection System maintenance tasks were identified as having a due date beyond their interval plus grace period as defined in ComEd's Protection System maintenance and testing program. ComEd discovered that a ComEd employee's keystroke error during a data entry resulted in a date change to certain preventive maintenance tasks for four batteries from a 2011 due date to a 2012 due date. Since work orders are generated automatically 45 days in advance of the due date based on these system tasks, ComEd did not timely generate the work orders for the four associated battery inspections and the devices were not maintained and tested within the defined intervals.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue implicated four of ComEd's 1,737 total batteries (0.23% of ComEd batteries) and 7,839 total Protection System devices (0.05% of all ComEd Protection System devices). ComEd performed all other battery maintenance and testing during the time frame of the issue. ComEd reviewed all available data during the timeframe of the issue and determined that no battery health concerns existed to pose a risk to the functionality and performance of the implicated batteries. Two of the implicated batteries, those batteries located at Station 22, were relatively new and ComEd's surveillance data indicated healthy new batteries. For these two Station 22 batteries, ComEd missed the quarterly inspections, but continued to perform all other battery maintenance during the timeframe of the issue. For the remaining two batteries, those batteries located at Station 16, ComEd performed other testing, during the timeframe of the issue, including annual and quarterly testing that were more rigorous than the missed 10-week inspections.	To mitigate this issue, ComEd: 1) conducted an initial preliminary investigation of maintenance inspection and testing tasks to confirm the continued reliability and safety of the Bulk Electric System; 2) immediately completed the identified outstanding tasks and implemented additional reporting, oversight and management controls; and 3) initiated an investigation to identify all issues and causal factors, implemented other necessary immediate remediation activities, defined a formal Mitigation Plan, and assigned appropriate corrective actions to assure full compliance for maintenance of all Protection System components.
Reliability*First* Corporation (Reliability*First)*	Delaware City Refining Company LLC (DCR)	NCR11173	RFC2012011201	VAR-002-1.1b	R1	On October 1, 2012, DCR submitted a Self-Certification to Reliability*First* stating that, as a Generator Operator and Generator Owner, it had an issue with VAR-002-1.1b R1. Certain of DCR's generators did not always operate in automatic voltage control mode and DCR failed to notify its Transmission Operator (TOP), PJM Interconnection (PJM), of the manual voltage control mode operation as required by VAR-002-1.1b. Specifically, DCR operates four of its steam generators in manual voltage control mode, in order to increase stability of those units. Historically, DCR has found that this manual voltage control mode has provided greater stability than operating the exciters in automatic voltage control mode, in which voltages exhibited large oscillations between the machines. These four generators are directly connected to the same 13.8 kV bus without any isolation transformers, unlike DCR's two combustion turbine generators, which are effectively controlled by automatic voltage regulation. DCR has operated these steam generators in manual voltage control mode since it acquired the plant and restarted it from an idle state in 2011. Operators control voltage by adjusting transformer taps and adjusting generator exciter output.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). DCR's operation of its steam generators in manual voltage control mode contributes to the stability of those generators and overall BPS stability and reliability. DCR subsequently agreed with its TOP that it should continue to operate in manual control mode, indicating that this operating mode was proper. Finally, DCR's primary purpose for generating electricity is to ensure the reliable operation of the refinery itself.	To mitigate this issue, DCR obtained an agreement with PJM to operate in manual control mode until further notice. DCR contacted PJM in September 2012 and obtained an agreement to operate in manual voltage control mode until further notice, pursuant to PJM's *Manual 14D*. PJM *Manual 14D* addresses generator operational requirements. It states that generators shall be operated with automatic voltage regulators in service, with exceptions for outages. PJM is considering the condition of these generators a submitted outage by DCR.
Reliability*First* Corporation (Reliability*First)*	Delaware City Refining Company LLC (DCR)	NCR11173	RFC2012011202	VAR-002-1.1b	R3	On October 1, 2012, DCR submitted a Self-Certification to Reliability*First* stating that, as a Generator Operator and Generator Owner, it had an issue with VAR-002-1.1b R3. Certain of DCR's generators did not always operate in automatic voltage control mode and DCR failed to notify its Transmission Operator (TOP), PJM Interconnection (PJM), of the change in status to manual voltage control mode operation as required by VAR-002-1.1b. Specifically, DCR operates four of its steam generators in manual voltage control mode, in order to increase stability of those units. Historically, DCR has found that this manual voltage control mode has provided greater stability than operating the exciters in automatic voltage control mode, in which voltages exhibited large oscillations between the machines. These four generators are directly connected to the same 13.8 kV bus without any isolation transformers, unlike DCR's two combustion turbine generators, which are effectively controlled by automatic voltage regulation. DCR has operated these steam generators in manual voltage control mode since it acquired the plant and restarted it from an idle state in 2011. Operators control voltage by adjusting transformer taps and adjusting generator exciter output.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). DCR's operation of its steam generators in manual voltage control mode contributes to the stability of those generators and overall BPS stability and reliability. DCR subsequently agreed with its TOP that it should continue to operate in manual control mode, indicating that this operating mode was proper. Finally, DCR's primary purpose for generating electricity is to ensure the reliable operation of the refinery itself.	To mitigate this issue, DCR obtained an agreement with PJM to operate in manual control mode until further notice. DCR contacted PJM in September 2012 and obtained an agreement to operate in manual voltage control mode until further notice, pursuant to PJM's *Manual 14D*. PJM *Manual 14D* addresses generator operational requirements. It states that generators shall be operated with automatic voltage regulators in service, with exceptions for outages. PJM is considering the condition of these generators a submitted outage by DCR.

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)*	PPL Holtwood, LLC (PPL Holtwood)	NCR00886	RFC2013012101	PRC-005-1b	R2	On February 11, 2013, PPL Holtwood submitted a Self-Report to Reliability*First* that, as a Generator Owner, it had an issue with PRC-005-1b R2. In 2011, PPL Generation, LLC, PPL Holtwood's parent company, established a separate relay test group as the group responsible for relay protection at all of the Eastern Fossil & Hydro group subsidiaries, including PPL Holtwood. In December 2012, the relay test group conducted a review to compare a database developed with information used to track testing prior to January 2012. During this review, the relay test group discovered that PPL Holtwood failed to perform maintenance and testing on one relay within the defined interval. The defined interval for this relay is six years with a 10% grace period. PPL Holtwood last performed maintenance and testing on this relay on September 28, 2011, therefore testing was due May 3, 2012. On December 18, 2012, the relay test group identified this missing maintenance and testing, and on December 19, 2012, PPL Holtwood performed maintenance and testing on this relay. When PPL Holtwood performed maintenance and testing on this relay, which constitutes one of PPL Holtwood's 237 relays, PPL Holtwood determined that the relay was functioning properly. The relay test group discovered no additional relays with missing maintenance and testing. This missed maintenance and testing occurred prior to the relay test group's monitoring of PPL Holtwood's maintenance and testing of relays.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. PPL Holtwood has alarming in place for certain of its Protection System devices. The primary and backup lockout relays alarm in the control room by lighting indicating lights labeled as "Primary Lockout Trip" and "Backup Lockout Trip." The span differential protection and exciter trouble alarms are also wired to the control room as well as numerous transformer variables such as winding temperature and oil level. In addition, PPL Holtwood has backup relay protection on the generator buses and generator step-up transformers. Furthermore, the misoperation of this relay would affect only one 12 MW hydro generator. When PPL Holtwood performed maintenance and testing on this relay, it discovered the relay to be in working condition.	To mitigate this issue, PPL Holtwood performed maintenance and testing on the relay.
Reliability*First* Corporation (Reliability*First)*	Eagle Point Power Generation, LLC (Eagle Point)	NCR11228	RFC2012010770	FAC-008-1	R1	On July 1, 2012 Eagle Point submitted a Self-Report to Reliability*First* stating that, as a Generator Owner, it had an issue with FAC-008-1 R1. The Facility Ratings methodology for Eagle Point did not include a statement that a Facility Rating shall equal the most limiting applicable equipment rating of the individual equipment that comprises that facility, as required by FAC-008-1 R1.1. In addition, the Facility Ratings methodology for Eagle Point did not include the following equipment as required by FAC-008 R1.2.2: relay protective devices; terminal equipment; and series and shunt compensation devices. Finally, the Facility Ratings methodology for Eagle Point did not include the source of the Facility Ratings. Specifically, the Facility Ratings methodology did not document the consideration of Facility Ratings provided by equipment manufacturers (FAC-008-1 R1.3.1), design criteria (FAC-008-1 R1.3.2), ambient conditions (FAC-008-1 R1.3.3), operating limitations (FAC-008-1 R1.3.4), and other assumptions (FAC-008-1 R1.3.5).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The steam turbine generator has been and continues to be the most limiting element of the Facility.	To mitigate this issue, Eagle Point 1) hired a qualified electrical engineering consultant to provide technical expertise in reviewing Facility Rating documentation. The consultant completed a review of equipment lists and inserted omitted equipment and equipment descriptions. The consultant also established documented Facility Ratings for all equipment; and 2) reviewed the consultant documentation, determined the final Facility Rating, and provided it to appropriate entities for review.
Reliability*First* Corporation (Reliability*First)*	Eagle Point Power Generation, LLC (Eagle Point)	NCR11228	RFC2012010771	FAC-009-1	R1	On July 1, 2012 Eagle Point submitted a Self-Report to Reliability*First* stating that, as a Generator Owner, it had an issue with FAC-009-1 R1. Eagle Point did not have Facility Ratings for relay protective devices, terminal equipment, and series and shunt compensation devices, as required by FAC-009-1 R1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The steam turbine generator has been and continues to be the most limiting element of the Facility.	To mitigate this issue, Eagle Point: 1) hired a qualified electrical engineering consultant to provide technical expertise in reviewing Facility Rating documentation. The consultant completed a review of equipment lists and inserted omitted equipment and equipment descriptions. The consultant also established documented Facility Ratings for all equipment; and 2) reviewed the consultant documentation, determined the final Facility Rating, and provided it to appropriate entities for review.
Reliability*First* Corporation (Reliability*First)*	Eagle Point Power Generation, LLC (Eagle Point)	NCR11228	RFC2012010772	FAC-008-1	R2	On July 1, 2012 Eagle Point submitted a Self-Report to Reliability*First* stating that, as a Generator Owner, it had an issue with FAC-008-1 R2. On June 8, 2012, Eagle Point's Transmission Operator (TOP) requested its Facility Ratings methodology. Eagle Point was unable to provide its TOP with a complete Facility Ratings methodology document because it was still in the process of determining whether the December 19, 2011 Facility Ratings methodology was accurate.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. To the best of Eagle Point's knowledge, no other entity had previously requested its Facility Ratings Methodology, therefore this was an isolated incident. In addition, when Eagle Point was able to provide the TOP with the methodology document, the TOP indicated it was no longer necessary, reducing the likelihood that this issue would have resulted in a reliability impact. The reason Eagle Point could not provide a complete methodology was because it was verifying the accuracy of the methodology, which demonstrates that Eagle Point had awareness of the issue and was working to address all facility ratings methodology issues.	To mitigate this issue, Eagle Point: 1) hired a qualified electrical engineering consultant to provide technical expertise in reviewing Facility Rating documentation. The consultant completed a review of equipment lists and inserted omitted equipment and equipment descriptions. The consultant also established documented Facility Ratings for all equipment; and 2) reviewed the consultant documentation, determined the final Facility Rating, and provided it to appropriate entities for review.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
ReliabilityFirst Corporation (ReliabilityFirst)	Eagle Point Power Generation, LLC (Eagle Point)	NCR11228	RFC2012010774	PRC-005-1	R1	On July 1, 2012 Eagle Point submitted a Self-Report to ReliabilityFirst stating that, as a Generator Owner, it had an issue with PRC-005-1 R1. Although Eagle Point has in place a Protection System maintenance and testing program for Protection System devices, the program does not include maintenance and testing intervals and their basis for voltage and current sensing devices and direct current control circuitry.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Eagle Point is interconnected by two separate and completely redundant 230 kV feeds from the same interconnection location. Eagle Point also has a backup battery system to supply power to the relays in the event of a failure. In addition, Eagle Point has an alarm system in place that alerts to the control room. Until May 3, 2012, Eagle Point was registered on the NERC Compliance Registry as Sunoco Power Generation LLC (Sunoco). On April 2, 2012, this facility was sold to Thunderbird Power Holdings, LLC, and the new facility name is Eagle Point. Eagle Point discovered this issue in its reviews after purchasing the facility. To the best of Eagle Point's knowledge, maintenance and testing on all relays was performed within their defined maintenance and testing intervals prior to Eagle Point owning the facility.	To mitigate this issue, Eagle Point 1) hired a qualified electrical engineering consultant to review Sunoco documents, establish a fully consolidated maintenance and testing program, and analyze for gaps in the maintenance under that program; 2) transferred the computerized maintenance management system data from the Sunoco system to the Eagle Point system and reviewed that data and any paper data from Sunoco; and 3) established a consolidated Protection System maintenance and testing program, compared that program to the previous program, and performed a gap analysis to determine a schedule for completing all maintenance and testing pursuant to that program.
ReliabilityFirst Corporation (ReliabilityFirst)	Eagle Point Power Generation, LLC (Eagle Point)	NCR11228	RFC2012010769	COM-002-2	R1	On July 1, 2012 Eagle Point submitted a Self-Report to ReliabilityFirst that, as a Generator Owner, it had an issue with COM-002-2 R1. The list of communications for the Eagle Point facility did not include a complete list of all voice communications, including cell phones, and data communications, including email and internet communication.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Since April 2, 2012, Eagle Point had some communications in place, which were staffed and available for addressing a real-time emergency condition at all times. Prior to April 2, 2012, Eagle Point was under different ownership, so Eagle Point is not knowledgeable regarding staffing.	To mitigate this issue, Eagle Point 1) completed the installation of a new telephone system that includes a PJM Interconnection hotline number; and 2) completed installation of the data and network system, revised the communications list and diagram to reflect the new telephone numbers and data communications, notified appropriate entities of the communication changes for emergency communication, and established a procedure for operators indicating when they should notify appropriate entities due to disruption or possible disruption of communication paths.
ReliabilityFirst Corporation (ReliabilityFirst)	Northern Indiana Public Service Company (NIPSCO)	NCR02611	RFC2011001250	PRC-008-0	R2	On November 29, 2011, NIPSCO submitted a Self-Report to ReliabilityFirst stating that, as a Transmission Owner, it had an issue with PRC-008-0 R2. NIPSCO discovered that it inadvertently entered a six-year maintenance and testing interval, rather than the two year interval required by its Under Frequency Load Shedding (UFLS) program, into its relay tracking system database for eight UFLS relays. As a result, NIPSCO did not test or maintain the eight UFLS relays within its UFLS program's two-year interval. NIPSCO has 167 UFLS relays on its system.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The eight relays at issue are microprocessor-based and perform self-testing and alarming. Additionally, all eight relays are monitored by NIPSCO through its distribution management system, which notifies operators of any alarms associated with the relays. Finally, upon performing maintenance and testing on the eight UFLS relays at issue, NIPSCO determined that each relay was set properly and would have responded correctly to an under frequency event.	To mitigate this issue, NIPSCO: 1) performed maintenance and testing on the eight UFLS relays at issue; and 2) assigned the UFLS relays at issue the correct two-year interval in its Relay Tracking System database. On June 14, 2012, ReliabilityFirst verified NIPSCO successfully completed the mitigation plan in accordance with its terms and conditions.
ReliabilityFirst Corporation (ReliabilityFirst)	Northern Indiana Public Service Company GO GOP (NIPSCO)	NCR02610	RFC2012010009	PRC-005-1	R1	From December 6, 2011 through December 13, 2011, ReliabilityFirst conducted a Compliance Audit. ReliabilityFirst identified that NIPSCO, as a Generator Owner, had an issue with PRC-005-1 R1. NIPSCO did not address DC Control circuitry in its Protection System maintenance and testing program (Program). Therefore, NIPSCO did not include the maintenance and testing interval and a basis for DC control circuitry or a summary of maintenance and testing procedures for DC control circuitry in 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. This issue is a documentation error. It is a documentation error because NIPSCO was conducting functional tests of its DC control circuitry for the duration of the issue. NIPSCO added DC control circuitry to its generator Program prior to ReliabilityFirst's Compliance Audit, however, the revised generator Program was not reviewed during the Compliance Audit because NIPSCO revised it after ReliabilityFirst's initial 90 day data request. Specifically, the generator relays utilize the DC control circuitry each time the unit is shut down, effectively testing DC control circuitry. On average, NIPSCO shuts down and restarts its generation units on average at least 10 times per year. ReliabilityFirst accepted NIPSCO's revised Program, which requires NIPSCO to test and maintain its DC control circuits on a six-year interval, as part of NIPSCO's Mitigation Plan. NIPSCO can provide logs for the circuits for each shutdown event which demonstrates that it performed functional tests of its DC control circuitry for the duration of the issue.	To mitigate this issue, NIPSCO: 1) revised its Program to include a maintenance and testing interval, a basis for the interval, and a summary of its maintenance and testing procedures for DC control circuitry; 2) will perform, on an ongoing basis, maintenance and testing described in its Program in conjunction with the functional testing performed when it shuts down and restarts its generating units. On December 26, 2012, ReliabilityFirst verified that NIPSCO completed the mitigation activities described in its Mitigation Plan.
ReliabilityFirst Corporation (ReliabilityFirst)	Northern Indiana Public Service Company (NIPSCO)	NCR02611	RFC2012010012	EOP-005-1	R4	From December 6, 2011 through December 13, 2011, ReliabilityFirst conducted a Compliance Audit. ReliabilityFirst identified that NIPSCO, as a Transmission Operator (TOP), had an issue with EOP-005-1 R4. NIPSCO did not coordinate its restoration plans with all the Generation Owners (GOs), specifically the Independent Power Producers (IPPs), within NIPSCO's area.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The IPPs within NIPSCO's area do not participate in NIPSCO's restoration plans. The IPPs in NIPSCO's area have no blackstart capability and cannot unilaterally inject energy onto the BPS. Furthermore, NIPSCO does not provide cranking power to any of the IPPs in its area as part of its restoration plans. Finally, NIPSCO coordinated its restoration plan with all non-IPP GOs, Balancing Authorities, and Reliability Coordinators in its area as well as neighboring TOPs.	To mitigate this issue, NIPSCO: 1) provided a redacted version of its System Restoration Plans to the IPPs within NIPSCO's area; and 2) provided all IPPs with the opportunity to view the complete System Restoration Plan upon request. On December 18, 2012, ReliabilityFirst verified that NIPSCO completed the mitigation activities described in its Mitigation Plan.

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)*	Northern Indiana Public Service Company (NIPSCO)	NCR02611	RFC2012010013	EOP-005-1	R7	From December 6, 2011 through December 13, 2011, Reliability*First* conducted a Compliance Audit. Reliability*First* identified that NIPSCO, as a Transmission Operator and Balancing Authority, had an issue with EOP-005-1 R7. NIPSCO did not verify each restoration procedure by testing or simulation. Specifically, NIPSCO did not verify that each restoration procedure that use intertie assistance were safe and effective in the restoration of its system. NIPSCO's primary restoration procedure is its black start procedure, which NIPSCO tested and verified pursuant to EOP-005-1 R7. However, NIPSCO included seven attachments to its black start procedure that consisted of restoration procedures using intertie assistance. Although NIPSCO did test and validate its primary intertie restoration procedure, it did not test the six other intertie restoration procedures.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. NIPSCO tested and verified its black start restoration procedure and primary intertie restoration procedure pursuant to EOP-005-1 R7. Additionally, following the Compliance Audit, NIPSCO verified all its intertie assistance restoration procedures by simulation. NIPSCO determined that each intertie restoration procedure was a viable restoration solution for its system and would have functioned as intended for the duration of the issue.	To mitigate this issue, NIPSCO verified by simulation that all previously unverified intertie assistance restoration plans are effective for the restoration of its system. On December 18, 2012, Reliability*First* verified that NIPSCO completed the mitigation activities described in its Mitigation Plan.
Reliability*First* Corporation (Reliability*First*)	LSP University Park, LLC (LSP University Park)	NCR11107	RFC2012010351	FAC-008-1	R1; R1.2	On May 11, 2012, LSP University Park, as a Generator Owner, self-reported an issue with FAC-008-1 R1. Due to an administrative oversight, LSP failed to include all required elements, as well as Normal and Emergency ratings, in its Facility Ratings Methodology. LSP University Park failed to address the following equipment in its Facility Ratings Methodology: transmission conductors, transformers, relay protective devices, terminal equipment, and series and shunt compensation devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that none of its generators could exceed the limitations of the most limiting element, which is the generator step-up transformer. Additionally, peak generation for the facility is below the limits established by both the original and revised ratings. Lastly, LSP University Park's revised Facility Ratings Methodology considers Normal and Emergency ratings to be equal.	To mitigate this issue, LSP University Park: 1) revised its Facility Ratings Methodology to include the missing equipment; and 2) modified its Facility Ratings Methodology to include both Normal and Emergency Ratings.
Reliability*First* Corporation (Reliability*First*)	LSP University Park, LLC (LSP University Park)	NCR11107	RFC2012010352	FAC-009-1	R1	On May 11, 2012, LSP University Park, as a Generator Owner, self-reported an issue with FAC-009-1 R1. LSP University Park failed to establish Facility Ratings that were consistent with its Facility Ratings Methodology.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that although LSP University Park's most limiting applicable equipment rating changed as a result of updating its Facility Ratings Methodology, that equipment component was included in the original Facility Ratings.	To mitigate this issue, LSP University Park updated its Facility Ratings to be consistent with its Facility Ratings Methodology.
Reliability*First* Corporation (Reliability*First*)	LSP University Park, LLC (LSP University Park)	NCR11107	RFC2012010353	PRC-005-1	R1	On May 11, 2012, LSP University Park, as a Generator Owner, self-reported an issue with PRC-005-1 R1. LSP University Park did not implement a fully-developed Protection System maintenance and testing program (Program) at facility registration.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that LSP University Park had been performing some maintenance and testing despite the absence of a formal Program. During a Compliance Audit, LSP University Park provided Reliability*First* with: records of testing and maintenance on station batteries in 2009 and 2012; testing and maintenance on relays in 2005 and 2009; and commissioning test records for instrument transformers in 2002.	To mitigate this issue, LSP University Park: 1) identified devices to be included in the Program; 2) researched and identified maintenance and testing intervals; 3) created summaries of maintenance and testing procedures; 4) reviewed and approved the Program; and 5) provided training on the Program to relevant personnel.
SERC Reliability Corporation (SERC)	Memphis Light, Gas and Water Division (MLGW)	NCR11066	SERC2012011167	EOP-005-1	R2	On September 28, 2012, MLGW submitted a Self-Report to SERC stating that, as a Transmission Operator (TOP), it had an issue with EOP-005-1 R2 because it failed to update its restoration plan at least annually for the year of 2012. MLGW reviewed its restoration plan during the 2010, 2011, and 2012 calendar years. During the restoration drill conducted on December 9, 2011, however, MLGW identified needed revisions to the restoration plan, including the addition of a new gate station which was expected to come online in May 2012. The summary of the restoration plan drill included a statement that the restoration plan should be reviewed and updated by May 2012 to include improvements and the new Collierville gate station. Because of delays, MLGW did not complete the new construction project until September 2012 and MLGW overlooked the established May 2012 date to revise the restoration plan. The December 9, 2011 restoration drill identified needed revisions to the restoration plan beyond the addition of the new gate station, including a change in the path used to re-energize the system from a gate to the interchange. Therefore, MLGW should have revised its restoration plan following the drill, regardless of the status of the delayed gate station.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Restoration of the MLGW transmission system is directed by Tennessee Valley Authority (TVA), MLGW's Reliability Coordinator, Balancing Authority, and adjacent TOP. Restoration requires re-energizing 115 kV and 161 kV network lines and load-serving substations. If MLGW's restoration efforts could not follow the prescribed path, TVA would direct circuit and load restoration through another path. MLGW does not have any blackstart resources in its TOP area and its restoration plan does not require cranking paths to restore station services to any other generators in its TOP area. MLGW transmission facilities are not part of any other TOP-defined cranking paths, whether for restoration of the Interconnection or restoring normal operations.	To mitigate this issue, MLGW: 1) updated its system restoration plan; and 2) enhanced its compliance management software and processes to better remind personnel of intended action dates. SERC has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	American Electric Power Service Corp. As Agent For Public Svc. Co. Of Oklahoma & SW Ele Pwr Co. (AEPW)	NCR01056	SPP20121011325	VAR-002-1.1b	R3; R3.1	On October 29, 2012, AEP submitted a Self-Report to SPP RE stating that, as a Generator Operator, it had an issue with VAR-002-1.b R3.1, because it did not report to its Transmission Operator (TOP) within 30 minutes the status change and expected duration of an outage of a power system stabilizer (PSS). At 2:51 a.m. on June 26, 2012, AEP's Stall 6S generator returned to service following a trip caused by loss of the unit's voltage regulator system. When the Stall generator returned to service the generator operators received a "PSS Control Enabled" alarm. In the investigation that immediately followed, it was determined that the alarm was activated when the PSS was disabled and the label for the alarm was not consistent with the PSS status. The PSS did not enable when the voltage regulator system was placed into service because of a diagnostic fault code indicating a mismatch between the primary and secondary control. Resetting the PSS cleared the fault and enabled the PSS. As a consequence of the faulty alarm, the generator operators were unaware that the PSS was disabled during the investigation, and thus did not notify the TOP of the PSS status change. The diagnostic fault code was reset and the PSS was returned to service at 10:15 a.m. on June 26, 2012.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was limited to the Stall S6 PSS, which was back in service within seven hours and twenty four minutes. Further, although the PSS was removed from service, the generator voltage was monitored and controlled by the generator operators, consistent with the required voltage schedule for the duration of PSS outage. Moreover, the issue did not cause any operating events or loss of load.	To mitigate the issue, AEP: 1) set the proper alarm code of the PSS; and 2) returned the PSS to service. SPP RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Borger Energy Associates, LP (Borger)	NCR01062	SPP2013012371	PRC-005-1	R2	On May 16, 2013, Borger, as a Generator Owner (GO), self-reported an issue with PRC-005-1 R2 because it had not tested or maintained all of its Protection System devices within the defined intervals set out in its Protection System maintenance and testing program (PSMTP). Specifically, Borger did not test 2 out of 70 instrument transformers during a 2010 testing of its substation Protection System devices. Borger has a total of 100 Protection System devices; therefore, Borger did not test 2% of its total Protection System devices. Borger completed testing of one instrument transformer in April 2011, and of the other in April 2013.	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 relays in which the two instrument transformers supply input are alarmed and monitored continuously by Borger operators. Failure of the instrument transformers would have resulted in a control room alarm. No alarms were recorded for these two instrument transformers for the duration of the issue, and the devices passed the maintenance and testing performed on them without any issues. Finally, Borger's size, a total plant capacity of 230 MW, further reduces risk to the BPS. A Settlement Agreement covering violations of PRC-005-1 R1 and PRC-005-1 R2 (SPP200900102 and SPP200900103) for Borger was filed with FERC under NP11-99-000 on January 31, 2011. On March 2, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. SPP RE determined that this issue is appropriate for FFT treatment because Borger has demonstrated improvements since its prior violations in 2009. The 2009 PRC-005-1 violations were discovered during a Compliance Audit. The violations were for not having a Protection System maintenance and testing program and for not testing any of its PRC-005-1 devices. Since that time, Borger mitigated the PRC-005-1 R1 violation, and tested almost all of its PRC-005-1 devices, and only failed to include the two at issue because of confusion in its instrument transformer inventory. Furthermore, the fact that Borger self-reported speaks to Borger's improvements in compliance.	To mitigate this issue, Borger: 1) performed testing and maintenance on the two instrument transformers that had not been tested in 2010; and 2) revised its Protection System inventory to include the two instrument transformers to prevent any future testing and maintenance confusion. SPP RE has verified the completion of all mitigation activity.
Southwest Power Pool Regional Entity (SPP RE)	Oklahoma Gas & Electric Company Co. (OGE)	NCR01130	SPP201100546	PRC-005-1	R2; R2.1; R2.2	On April 15, 2011, OGE, as a Generator Owner, self-reported an issue with PRC-005-1 R2 because it could not locate documentation that it had implemented its maintenance and testing program for all of its generation Protection System devices, namely: batteries, DC circuitry, and relays. OGE did not have documentation for annual station battery bank tests for 14 generating units, at 4 generating stations, from 2008 to 2010. OGE had documentation of 89% of the required monthly station battery bank inspections and 88% of the required quarterly station battery bank inspections at 3 of the 4 generating stations during that time period. There was no documentation of monthly station battery bank inspections for the fourth generating station; instead, OGE provided closed work orders from its Systems Applications and Products in Data Processing (SAP) system, which showed that 22% of the monthly battery bank inspections occurred in the time period from 2008 to 2010. Additionally, OGE had not tested DC circuitry or relays at its Horseshoe Lake Generating Station A-1 Unit during the same time frame. In all, no more than 20% of OGE's Protection System devices were affected by this issue. Subsequently, during a Compliance Audit from April 18 through April, 21 2011, SPP RE discovered a number of relay tests that OGE had performed in which the test results were marked as "failed" in the "as left" portion of the test. OGE could not provide documentation to demonstrate that it took corrective action to address the "failed" relays.	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 OGE failed to keep documented records of annual testing for 14 generating units, OGE did have several documented monthly and quarterly inspections, along with documented SAP work orders, to evidence that OGE was performing some testing and maintenance on its station batteries. Additionally, OGE was continuously monitoring all of its batteries during the duration of the issue via its Energy Management System. 2) although OGE did not test DC circuitry or relays at its Horseshoe Lake Generating Station A-1 unit, the unit had a nameplate generating capacity of 2.5 MW. Furthermore, this unit was not directly connected to the BPS; instead, it was connected to, and capable of, supplying power to a gas turbine designated as a blackstart resource. 3) only 12 of 146 relay test results that SPP RE reviewed (8%) were left in a "failed" state. OGE was able to provide evidence explaining these 12 "failures." OGE used the same series of tests for all of its relays and in doing so, it tested for functions that were not applicable to some relays. Because the non-applicable functions automatically appeared as a failed item, 12 relays showed a "failed" state after testing. The functions that these 12 relays were set to perform were retested and functioned properly.	To mitigate this issue, OGE: 1) revised its Instructions and Methods for maintenance and testing (I&M) to make its procedures clearer to affected personnel, including expressly referencing PRC-005 in the I&M and incorporating specific recordkeeping requirements and checklist forms for employees; 2) used its revised I&M to test the equipment associated with its generating stations. All testing is now up-to-date; 3) developed a process for identifying and documenting equipment left in an "as-left failed" status, including reasons why the equipment is left in a "failed" state, using pre-defined failure codes; and 4) trained supervisors on all new processes and procedures. SPP RE has verified the completion of all mitigation activity.
Texas Reliability Entity (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	TRE2012011184	VAR-002-1.1b	R1	On August 31, 2012, AEP self-certified to Texas RE that as a Generator Operator, it had an issue with VAR-002-1.1b R1. Specifically, on February 16, 2012 at 3:30 p.m. Central Standard Time (CST), AEP switched the voltage control mode of the Automatic Voltage Regulator (AVR) at its Oklaunion generation plant from automatic to manual without notifying the Transmission Operator (TOP). AEP has an issue with VAR-002-1.1b R1 from February 16, 2012 when the AVR was switched to manual, to February 18, 2012 when the AVR was set to automatic and the TOP was notified.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) due to the following factors: a) the TOP was aware that the AVR was being tuned and going in and out of service; b) the issue period was approximately 35 hours; c) voltage on the Oklaunion facility was being monitored by AEP; d) the unit maintained its established voltage limits during the issue period; e) during the issue period the Oklaunion facility was fully available and no trips occurred; f) the BPS was not under stress. A Find, Fix, Track and Report (FFT) informational filing addressing remediated issues for certain registered entities including noncompliance with VAR-002-1.1a R1 (SPP201000431) for AEP with the Southwest Power Pool Regional Entity region was filed with FERC under RC12-13-000 on June 29, 2012. The 60-day review period passed on August 28, 2012. A Settlement Agreement covering two violations of VAR-002-1.1b R1 and R3 (RFC2011001111 and RFC201100130) for AEP within the Reliability*First* Corporation region was filed with FERC under NP12-27-000 on May 30, 2012. On June 29, 2012, FERC issued an order stating it would not engage in further review of the Notice of Penalty. Texas RE determined that the instant issue is appropriate for FFT treatment because it is AEP's first VAR-002 violation in the Texas RE region. Also, the instant issue involved the commissioning of a new facility.	To mitigate this issue, AEP: 1) placed the facility's AVR in auto mode; and 2) notified the TOP. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	GIM Channelview Cogeneration LLC (GIM Channelview)	NCR00292	TRE201100461	PRC-004-1	R3	During a September 14, 2011 Compliance Audit, Texas RE determined that GIM Channelview, as a Generator Owner, had an issue with PRC-004-1 R3. GIM Channelview failed to report to the Regional Reliability Organization (RRO) misoperation when one of its units had a fuse failure and trip on May 22, 2010. Analysis indicated the misoperation to be an unintentional Protection System operation when no fault or other abnormal condition had occurred unrelated to on-site maintenance and testing activity. The failure was caused by a defective fuse on the C-phase potential transformer. The analysis and corrective action plans for this misoperation were not provided to the RRO, the Electric Reliability Council of Texas (ERCOT). The duration of the issue was from May 22, 2010, the date of the misoperation analysis, until September 25, 2011, the date GIM Channelview met the requirement language of the new Standard Version .	This violation posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because GIM Channelview did take corrective action at the time of the incident. GIM Channelview replaced the defective fuse on the C-phase potential transformer, and conducted a root cause analysis. The entity also immediately documented the analyses including root causes and corrective action plans of the incident.	To mitigate this issue GIM Channelview provided analysis and corrective action plan during the Compliance Audit. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	GIM Channelview Cogeneration LLC (GIM Channelview)	NCR00292	TRE201100462	PRC-005-1	R2	During a September 14, 2011 Compliance Audit, Texas RE determined that GIM Channelview, as a Generator Owner, had an issue with PRC-005-1 R2. Two relays were not tested within the program intervals. Testing was due on July 1, 2008 but the relays were not tested until February 22, 2010. GIM Channelview provided evidence that the Protection System devices were maintained and tested within the defined intervals and the date when each Protection System device was last tested and maintained. All requests for Protection System information were satisfied with the exception of two relays. For the two relays, test records were provided showing testing was last performed on February 22, 2010. GIM Channelview provided a 2008 tracking spreadsheet which shows these two relays were previously tested in April 2004. This testing interval (5 years and 10 months) exceeds the program interval of 4 years (with the provision that if maintenance interval exceeds 4 years, then maintenance must be performed during the next unit outage). GIM Channelview was not able to provide any records to demonstrate these two relays were tested within the program interval. GIM Channelview had a total of 172 devices, the two untested relays equaled 1.16% of that amount. The duration of the issue was from July 1, 2008, when the testing was due, until February 22, 2010, the date the last relay was tested.	The violation posed a minimal risk and did not pose a serious or substantial risk to the bulk power system and had a minimal risk. The two relays were tested outside of the defined testing interval by about 20 months. GIM Channelview had records from 2004 showing testing was completed. However, GIM Channelview was not registered until July 1, 2008. When the relays were tested in 2010, the test results were satisfactory. The two relays represented 1.16% of the total devices in the program.	To mitigate this issue GIM Channelview tested the two relays. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Papalote Creek II, LLC (Papalote)	NCR11033	TRE2012009902	VAR-002-1.1b	R3	On January 26, 2012, Papalote submitted a Self-Report to Texas RE stating that, as a Generator Owner and Generator Operator (GOP), it had an issue with VAR-002-1.1b R3. Texas RE has reviewed the evidence submitted and has determined that between May 18, 2010 to November 1, 2010, Papalote experienced 12 instances where a change in Automatic Voltage Regulator (AVR) status was not communicated to its Transmission Operator (TOP), the Electric Reliability Council of Texas (ERCOT). The failure to notify the TOP was due to technical communication issues between a third party contractor, which was performing some GOP functions for Papalote, including communicating the AVR status, and ERCOT.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because at no time during the issue period did Papalote experience any voltage issues with its systems. Furthermore, Papalote operators were continuously monitoring voltage levels and were supported by alarms, which trigger when deviations from voltage profile limits occur. Finally, the unit was still able to provide the voltage support needed during the pendancy of the issue.	To mitigate this issue: 1) as of December 1, 2011, EON Climate and Renewables (EC&R) (Papalote Creek II's parent company) has taken over all GOP functions and no longer depends on a third party contractor for communications with ERCOT. Texas RE has verified that EC&R has been communicating statuses of its facilities to ERCOT, and EC&R has verified that it has not experienced any other instances where it failed to communicate its status; and 2) EC&R has updated its procedures to reflect its responsibility for communicating any changes in reactive capability to the TOP. EC&R has also reviewed these procedures with its operators to ensure that they are aware of their role in these procedures. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	City of Austin dba Austin Energy (AE)	NCR04030	TRE201100476	PRC-005-1	R1; R1.1; R1.2	On September 30, 2011, AE submitted a Self-Report, as a Generator Owner, citing an issue with PRC-005-1 R1.1 and R1.2. AE failed to clearly define maintenance and testing intervals and their basis for all of the components. Specifically, AE did not include voltage or current sensing devices, DC control circuitry, and battery testing in its maintenance and testing program. AE failed to include 94 out of 333 devices (28%) in its maintenance and testing program. The duration of the issue was from June 28, 2007, when the Standard become mandatory and enforceable, through December 20, 2011, when the issue was mitigated.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because AE stated in its Self-Report and a response to Texas RE questions that testing was completed but AE did not document the evidence of this testing. AE provided an attestation stating that the facilities involved are staffed 24 hours a day and if any issues had occurred, plant staff would have been able to immediately address any operational issues. No generating unit outage, equipment failure, or confirmation of any current and voltage sensing misoperation occurred during the period of the issue. A Settlement Agreement covering three violations for AE of Reliability Standards PRC-005-1 R1, PRC-005-1 R2, and PRC-008-0 R2 was filed with FERC under NP12-18-000 on February 29, 2012. On March 30, 2012, FERC issued an order stating it would not engage in further review of the Notice of Penalty. The prior violations were similar to this instance of noncompliance but pertained AE's Distribution Provider and Transmission Owner functions (NERC Registration ID: NCR04029) for the period from June 28, 2007 through July 27, 2010. Texas RE determined that the instant issue is appropriate for FFT treatment because it occurred around the same time as the violations for NCR04029, and thus should not be considered a repeat instance of noncompliance.	To mitigate this issue, AE: 1) reviewed all aspects of its Protection System maintenance program for its generation assets to ensure that all requirements of PRC-005 are covered; and 2) created a new full-time position in December 2010 that resides within the Power Supply and Market Operations (PSMO) business unit. The PSMO quality and compliance manager focuses on the compliance activities of the PSMO and serves as a primary liaison to the reliability compliance office (RCO) and works closely with the RCO to monitor the Reliability Requirements applicable to AE's generation-related business units. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	City of Austin dba Austin Energy (AE)	NCR04030	TRE201100477	PRC-005-1	R2; R2.1; R2.2	On September 30, 2011, AE, as a Generator Owner, submitted a Self-Report citing an issue with PRC-005-1 R2.1 and R2.2. AE failed to provide evidence that all of its Protection System devices were maintained and tested within the defined intervals, which presented an issue with R2.1. In addition, AE did not include the date these systems were last tested and maintained, as required in R2.2. Texas RE determined that AE did not maintain and test 26% of its protective relays, 24% of its voltage and current sensing devices, and 66% of its DC control circuitry. This issue was from June 28, 2007, the date the Standard become mandatory and enforceable, through September 12, 2012, when was the issue mitigated.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because AE states that testing was completed but did not document the evidence of this testing. AE provided an attestation stating that the facilities involved are staffed 24 hours a day and if any issues had occurred, plant staff would have been able to immediately address any operational issues. In addition, AE does not have any associate communication systems, the omission of the device type was not significant. Additionally, no generating unit outage, equipment failure, or confirmation of any current and voltage sensing misoperation occurred during the period of the issue. A Settlement Agreement covering violations pertaining to Reliability Standards PRC-005-1 R1, PRC-005-1 R2, and PRC-008-0 R2 was filed with FERC under NP12-18-000 on February 29, 2012. On March 30, 2012, FERC issued an order stating it would not engage in further review of the Notice of Penalty. The prior violations were similar to this instance but pertained to the Distribution Provider and Transmission Owner functions (NERC Registration ID NCR04029) for the period from June 28, 2007 through July 27, 2010. Texas RE determined that the instant issue is appropriate for FFT treatment because it occurred around the same time as the violations for NCR04029, and thus should not be considered a repeat instance of noncompliance.	To mitigate this issue, AE performed maintenance and testing of all relevant equipment and performed quality assurance and quality check of relevant data. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Equistar Chemical, LP (Equistar)	NCR04055	TRE2012010270	PRC-005-1	R1	During a Compliance Audit conducted from May 15, 2012 through March 17, 2012, Texas RE discovered that Equistar, as a Generator Owner, had an issue with PRC-005-1 R1. Equistar did not have maintenance and testing intervals and their basis for DC circuits and communications. Equistar also failed to provide a basis for adjusting the intervals for its relay maintenance and testing when it updated the document that described the maintenance and testing program intervals in 2011 from the previous version in 2006. Equistar had an issue with PRC-005-1 R1 from June 28, 2007, the date the Standard became mandatory and enforceable, through August 10, 2012, the date Equistar developed intervals and basis for testing.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The following factors mitigate the risk: 1) the nameplate rating of the plant is 45 MW but the chemical plant uses half of that capacity; normally, the cogen plant exports less than 10 MW to the Electric Reliability Council of Texas's market; 2) the only time Equistar exported more than 20 MW was during the unusually cold weather period in February 2011; 3) Equistar's policy is to perform maintenance on all the cogen devices during the chemical plant outages every two years and that is a short time frame for testing of plant equipment compared to industry standards; 4) Equistar has one communications circuit to a Transmission Owner (TO) substation it ties to 0.9 miles from the plant; and 5) If an issue did occur in Equistar's plant due to missed Protection System device maintenance and testing, the TO substation that Equistar ties with would have isolated it from the Bulk Electric System.	To mitigate this issue, Equistar: 1) created a site-specific basis document to define the intervals for testing and maintenance of the Protective System devices; 2) modified its maintenance procedures to reference a new maintenance guideline reliability procedure associated with this Standard; 3) created a new site-specific interval testing and basis document to include DC Circuit and communication system testing. Then modified maintenance procedures to reference new maintenance guideline in PRC-005 R1.
Texas Reliability Entity (Texas RE)	Equistar Chemical, LP (Equistar)	NCR04055	TRE2012010271	PRC-005-1	R2	During a Compliance Audit conducted from May 15, 2012 through March 17, 2012, Texas RE discovered that Equistar, as a Generator Owner, had an issue with PRC-005-1 R2. Equistar missed at least one maintenance and/or test for all of its Protection System devices except for Potential Transformers (PT) and Current Transformers (CTs), giving it a missing percentage of 70% from the total Protection Devices. The testing intervals for the following devices were as follows: the interval was 2 years for electromechanical relays. Equistar did not present maintenance and test results for testing required for 17 of the 18 (94.5%) electromechanical relays in 2007. Previous maintenance was in 2005 but results were next available in 2009. One of the 18 electromechanical relays (87L) had test results for 1996 and 2010. Test results DC circuits and communications systems were presented only for 2011. The test intervals for batteries were monthly and quarterly. There were four battery systems with missing monthly and quarterly results per the table below: -For 2011 - Missing 1 Monthly; 0 Quarterly -For 2010 - Missing 6 Monthly; 0 Quarterly -For 2009 - Missing 1 Monthly; 5 Quarterly -For 2008 - Missing 3 Monthly; 8 Quarterly -For 2007 (3rd and 4th Quarters) - Missing 2 Monthly; 8 Quarterly The duration of the issue was from June 28, 2007, when the Standard become mandatory and enforceable through April 7, 2011, when the last of the systems, the DC circuits and communication system, was maintained and tested.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The following factors mitigate the risk: 1) the nameplate rating of the plant is 45 MW but the chemical plant uses half of that capacity; normally, the cogen plant exports less than 10 MW to the Electric Reliability Council of Texas's market; 2) the only time Equistar exported more than 20 MW was during the unusually cold weather period in February 2011; 3) Equistar's policy is to perform maintenance on all the cogen devices during the chemical plant outages every two years and that is a short time frame for testing of plant equipment compared to industry standards; 4) Equistar has one communications circuit to a Transmission Owner (TO) substation it ties to 0.9 miles from the plant; and 5) if an issue did occur in Equistar's plant due to missed Protection System device maintenance and testing, the TO substation that Equistar ties with would have isolated it from the Bulk Electric System.	To mitigate this issue, Equistar: 1) created a site-specific basis document to define the intervals for testing and maintenance of the Protective System devices; 2) modified its maintenance procedures to reference a new maintenance guideline reliability procedure associated with this Standard; and 3) corrected the monthly battery Preventative Maintenance (PM) notice in its tracking system and emphasized to the involved personnel the need for the PM to be finished in that month as well as making sure that the records are moved to the proper electronic folder. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	CER - Colorado Bend Energy Partners LP (CBEC)	NCR110067	TRE201100528	PRC-005-1	R1; R1.1; R1.2	During a Spot-Check conducted from October 10, 2011 through October 14, 2011, Texas RE determined that CBEC, as a Generator Owner (GO), had an issue with PRC-005-1 R1.1 and R1.2. The documented generation Protection System maintenance and testing program that was in effect at the beginning of the enforceable period did not include maintenance and testing intervals and their basis or a summary of maintenance and testing procedures. Beginning on November 18, 2010, the next and subsequent versions of generation Protection System maintenance and testing programs included maintenance and testing intervals that either did not have a documented basis or were not consistent with the documented basis. The issues involved with the second and subsequent versions are limited to defective or missing bases. CBEC had an issue with PRC-005-1 R1.1 and R1.2 from August 17, 2010, the date of its registration as a GO, through May 10, 2013, the date the formal Mitigation Plan was completed.	Texas RE determined the issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. The initial maintenance and testing program lacked material specificity for a brief period of three months. The scope of the issue three months after registration was limited to defective basis, specifically support for the chosen maintenance and test intervals. Additionally, all generation Protection System maintenance and test intervals in the subsequent, substantive program issued November 18, 2010, or thereafter were more conservative or equal to the intervals recommended in the NERC Technical Reference “Maximum Verification Interval” maintenance and test intervals document.	To mitigate this issue, CBEC: 1) updated its Maintenance and Testing procedure to include maintenance and testing intervals and their basis. The procedure was revised to align with engineering practices derived from specific sections of the PJM Interconnection's relevant documents; and 2) implemented the procedure by integrating it into the fleet’s NERC compliance program. All relevant personnel were required to review the procedure and implement all applicable changes by the compliance date. The integrated procedures were implemented in early 2013. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	CER - Colorado Bend Energy Partners LP (CBEC)	NCR110067	TRE201100529	PRC-005-1	R2; R2.1; R2.2	During a Spot-Check conducted from October 10, 2011 through October 14, 2011, Texas RE determined that CBEC, as a Generator Owner (GO), had an issue with Reliability Standard PRC-005-1 R2.1 and R2.2. Specifically, CBEC was either missing certain maintenance and test records or reflected exceeded required intervals. The issues involved 22 out of 54 devices or 40.74% of the total, involving relays and current transformers. CBEC had an issue with PRC-005-1 R2.1 and R2.2 from August 17, 2010, the date of its registration as a GO, through March 20, 2012, the date CBEC completed required maintenance and testing.	Texas RE determined the issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system for the following reasons: 1) although certain test records were missing, the plant was commissioned in 2007 and it was very likely that the subject equipment was in fact maintained and tested during the commissioning process; 2) although relays were not maintained and tested in a timely manner, the final intervals were considerably more conservative than the intervals recommended by the NERC Relay Maintenance Technical Reference; 3) the relays and current transformers were continuously monitored and CBEC would have learned of an equipment issue promptly, had one occurred; and 4) backup relaying was in place had primary systems failed.	To mitigate the issue, CBEC completed all maintenance and testing on undocumented and untimely tested Protection System elements. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	CER - Quail Run Energy Partners LP (QREC)	NCR110068	TRE201100535	PRC-005-1	R1; R1.1; R1.2	During a Spot-Check conducted from October 10, 2011 through October 14, 2011, Texas RE determined that QREC, as a Generator Owner (GO), had an issue with PRC-005-1 R1.1 and R1.2. The documented generation Protection System maintenance and testing program that was in effect at the beginning of the enforceable period did not include maintenance and testing intervals and their basis or a summary of maintenance and testing procedures. Beginning on November 18, 2010, the next and subsequent versions of generation Protection System maintenance and testing programs included maintenance and testing intervals that either did not have a documented basis or were not consistent with the documented basis. The issues involved with the second and subsequent versions are limited to defective or missing bases. QREC had an issue with PRC-005-1 R1.1 and R1.2 from August 17, 2010, the date of its registration as a GO, through May 10, 2013, the date the formal Mitigation Plan was completed.	Texas RE determined the issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system. The initial program lacked material specificity for a period of three months. The scope of the issue three months after registration was limited to defective basis, specifically support for the chosen maintenance and test intervals. Additionally, all generation Protection System maintenance and test intervals in the subsequent, substantive program issued November 18, 2010, or thereafter were more conservative or equal to the intervals recommended in the NERC Technical Reference “Maximum Verification Interval” maintenance and test intervals document.	To mitigate this issue, QREC: 1) updated its Maintenance and Testing procedure to include maintenance and testing intervals and their basis. The procedure was revised to align with engineering practices derived from specific sections of the PJM Interconnection's relevant documents; and 2) implemented the procedure by integrating it into the fleet’s NERC compliance program. All relevant personnel were required to review the procedure and implement all applicable changes by the compliance date. The integrated procedures were implemented by early 2013. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	CER - Quail Run Energy Partners LP (QREC)	NCR110068	TRE201100536	PRC-005-1	R2; R2.1; R2.2	During a Spot-Check conducted from October 10, 2011 through October 14, 2011, Texas RE determined that QREC, as a Generator Owner (GO), had an issue with PRC-005-1 R2.1 and R2.2. Specifically, QREC was either missing certain maintenance and test records or reflected exceeded required intervals. The issues involved 9 out of 58 devices or 15.51% of the total, involving relays and current transformers. QREC had an issue with PRC-005-1 R2.1 from August 17, 2010, the date of registration as a GO, through March 20, 2012, the date QREC completed the required maintenance and testing.	Texas RE determined the issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system for the following reasons: 1) although certain test records were missing, the plant was commissioned in 2007 and it was very likely that the subject equipment was in fact maintained and tested during the commissioning process; 2) although relays were not maintained and tested in a timely manner, the final intervals were considerably more conservative than the intervals recommended by the NERC Relay Maintenance Technical Reference; 3) the relays and current transformers were continuously monitored and QREC would have learned of an equipment issue promptly, had one occurred; and 4) backup relaying was in place had primary systems failed.	To mitigate the issue, QREC completed all maintenance and testing on undocumented and untimely tested Protection System elements. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	EC&R Panther Creek Wind Farm III, LLC (Panther Creek III Wind Farm)	NCR10334	TRE201100539	VAR-002-1.1a	R3	On November 2, 2011, Panther Creek III Wind Farm, as a Generator Operator (GOP), submitted a Self-Certification to Texas RE citing an issue with VAR-002-1.1a R3. Texas RE has reviewed the evidence submitted and has determined that from July 5, 2010 to November 10, 2010, Panther Creek III Wind Farm experienced six instances where it did not communicate a change in reactive capability to its Transmission Operator (TOP), the Electric Reliability Council of Texas (ERCOT). The failure to notify its TOP were due to a general failure of its operators to communicate the change in reactive capability status.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Panther Creek III operators were continuously monitoring voltage levels, supported by alarms set to trigger on deviations away from voltage profile limits. At no time during the issue period did Panther Creek III experience any voltage issues with their systems.	To mitigate this issue: 1) as of December 1, 2011, EON Climate and Renewables (EC&R) (Panther Creek III Wind Farm’s parent company) has taken over all GOP functions and no longer depends on a third-party contractor for communications with ERCOT. Texas RE has verified EC&R has been communicating statuses of its facilities to ERCOT, and EC&R has verified that it has not experienced any other instances where it failed to communicate its status to ERCOT; and 2) EC&R has updated its procedures to reflect its responsibility for communicating any changes in reactive capability to the TOP. EC&R has also reviewed these procedures with its operators to ensure that they are aware of their role in these procedures. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	EC&R Panther Creek Wind Farm I & II, LLC (Panther Creek I & II Wind Farm)	NCR10249	TRE201100541	VAR-002-1.1a	R3	On November 2, 2011, Panther Creek I & II Wind Farm, as a Generator Operator (GOP), submitted a Self-Certification to Texas RE citing an issue with VAR-002-1.1a R 3. Texas RE has reviewed the evidence submitted and has determined that on July 29, 2010 Panther Creek I & II Wind Farm experienced one instance where it did not communicate a change in reactive capability to its Transmission Operator (TOP), the Electric Reliability Council of Texas (ERCOT). The failure to notify its TOP was due to a general failure of its operators to communicate the change in reactive capability status.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Panther Creek I & II operators were continuously monitoring voltage levels, supported by alarms set to trigger on deviations away from voltage profile limits. At no time during the issue period did Panther Creek I & II Wind Farm experience any voltage issues with their systems.	To mitigate this issue: 1) as of December 1, 2011, EON Climate and Renewables (EC&R) (Panther Creek 1 & 2 Wind Farm's parent company) has taken over all GOP functions and no longer depends on a third-party contractor for communications with ERCOT. Texas RE has verified EC&R has been communicating statuses of its facilities to ERCOT, and EC&R has verified that it has not experienced any other instances where it failed to communicate its status to ERCOT; and 2) EC&R has updated its procedures to reflect its responsibility for communicating any changes in reactive capability to the TOP. EC&R has also reviewed these procedures with its operators to ensure that they are aware of their role in these procedures. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Papalote Creek I, LLC (Papalote Creek I Wind Farm)	NCR10335	TRE201100537	VAR-002-1.1a	R3	On November 2, 2011, Papalote Creek I Wind Farm, as a Generator Operator (GOP), submitted a Self-Certification to Texas RE citing an issue with VAR-002-1.1a R3. Texas RE has reviewed the evidence submitted and has determined that from July 9, 2010 to October 6, 2010, Papalote Creek I Wind Farm experienced nine instances where it did not communicate a change in reactive capability its Transmission Operator (TOP), the Electric Reliability Council of Texas (ERCOT). The failures to notify the TOP were due to a general failure of its operators to communicate the change in reactive capability status.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Papalote Creek I operators were continuously monitoring voltage levels, supported by alarms set to trigger on deviations away from voltage profile limits. At no time during the issue period did Papalote Creek I experience any voltage issues with their systems.	To mitigate this issue: 1) as of December 1, 2011, EON Climate and Renewables (EC&R) (Papalote Creek 1 Wind Farm's parent company) has taken over all GOP functions and no longer depends on a third-party contractor for communications with ERCOT. Texas RE has verified EC&R has been communicating statuses of its facilities to ERCOT, and EC&R has verified that it has not experienced any other instances where it failed to communicate its status to ERCOT; and 2) EC&R has updated its procedures to reflect its responsibility for communicating any changes in reactive capability to the TOP. EC&R has also reviewed these procedures with its operators to ensure that they are aware of their role in these procedures. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Karnes Electric Cooperative, Inc. (KEC)	NCR10178	TRE2012010751	CIP-001-1	R1	During a July 24, 2012 through July 26, 2012 Compliance Audit of KEC as a Load Serving Entity, Texas RE discovered an issue with CIP-001-1 R1. KEC's electric service emergency operations plan manual did not have procedures that related directly to sabotage events. The manual mentioned sabotage and terrorist acts but did not specifically have procedure for recognition of sabotage events as required. The issue was from February 22, 2010, KEC's registration date through, May 11, 2011, the date the sabotage awareness and reporting procedures and guidelines manual that KEC provided was found to have adequate procedures to make its operating personnel recognize and be aware of sabotage events.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because KEC had an emergency plan in place at the time of registration, which made mention of sabotage covered certain emergency events, such as major terrorist events and vandalism. KEC also had a list of appropriate people to contact if the emergencies occurred, as defined by the previous procedure. KEC also attested that operators received some training in 2008 of the emergency plan in place. KEC also has a peak demand at approximately 65 MW.	To mitigate this issue, KEC created its sabotage awareness and reporting procedures and guidelines manual. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Karnes Electric Cooperative, Inc. (KEC)	NCR10178	TRE2012010766	CIP-001-1	R2	During a July 24, 2012 through July 26, 2012 Compliance Audit of KEC as a Load Serving Entity, Texas RE discovered an issue with CIP-001-1 R2. From February 22, 2010 through May 11, 2011, KEC's electric service emergency operations plan manual did not have procedures that related directly to communication of sabotage events. Texas RE found only vague guidelines for communicating emergencies. The sabotage awareness and reporting procedures and guidelines manual dated May 11, 2011 that KEC provided was found to have adequate communication procedures to communicate information to appropriate parties in the Interconnection.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because KEC had an emergency plan in place at the time of registration, which made mention of sabotage covered certain emergency events, such as major terrorist events and vandalism. KEC also had a list of appropriate people to contact if the emergencies occurred, as defined by the previous procedure. KEC also attested that operators received some training in 2008 of the emergency plan in place. KEC also has a peak demand at approximately 65 MW.	To mitigate this issue, KEC created its sabotage awareness and reporting procedures and guidelines manual. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Karnes Electric Cooperative, Inc. (KEC)	NCR10178	TRE2012010767	CIP-001-1	R3	During a July 24, 2012 through July 26, 2012 Compliance Audit of KEC as a Load Serving Entity, Texas RE discovered an issue with Reliability Standard CIP-001-1 R3. From February 22, 2010 through May 11, 2011, KEC's electric service emergency operations plan manual did not directly describe reporting of sabotage events. Additionally, KEC provided inadequate evidence to demonstrate it provided the guideline material to operating personnel. The sabotage awareness and reporting procedures and guidelines manual dated May 11, 2011 that KEC provided was found to have adequate guidelines for reporting disturbances, and was backed-up with training agenda and sign-in sheets of operating personnel.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because KEC had an emergency plan in place at the time of registration, which made mention of sabotage covered certain emergency events, such as major terrorist events and vandalism. KEC also had a list of appropriate people to contact if the emergencies occurred, as defined by the previous procedure. KEC also attested that operators received some training in 2008 of the emergency plan in place. KEC also has a peak demand at approximately 65 MW.	To mitigate this issue, KEC created its sabotage awareness and reporting procedures and guidelines manual. Texas RE has verified the completion of all mitigation activity.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	Karnes Electric Cooperative, Inc. (KEC)	NCR10178	TRE2012010768	CIP-001-1	R4	During a July 24, 2012 through July 26, 2012 Compliance Audit of KEC as a Load Serving Entity, Texas RE discovered an issue with CIP-001-1 R4. From February 22, 2010 through May 11, 2011, KEC's electric service emergency operations plan manual did not have procedures for reporting information to local FBI. KEC did not show evidence that communications were established with local FBI prior to the implementation of KEC's CIP-001 Manual. The sabotage awareness and reporting procedures and guidelines manual dated May 11, 2011 that KEC provided was found to have adequate procedures to report information to local FBI, and an e-mail was provided that showed communication with local FBI officials.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because KEC had an emergency plan in place at the time of registration, which made mention of sabotage covered certain emergency events, such as major terrorist events and vandalism. KEC also had a list of appropriate people to contact if the emergencies occurred, as defined by the previous procedure. KEC also attested that operators received some training in 2008 of the emergency plan in place. KEC also has a peak demand at approximately 65 MW.	To mitigate this issue, KEC created its sabotage awareness and reporting procedures and guidelines manual. Texas RE has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Silicon Valley Power (SNCL)	NCR05392	WECC2012011508	CIP-001-1	R2	On December 13, 2012, SNCL submitted a Self-Report to WECC stating that, as a Generator Operator, Load Serving Entity, and Transmission Operator, it had an issue with CIP-001-1 R2. Specifically, SNCL had one outdated email address for one of its contacts. WECC determined that SNCL failed to update procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although SNCL's reporting procedures did not contain the correct email address for the WECC Reliability Coordinator (RC), SNCL's electric control center still maintained current contact information for appropriate parties in the Interconnection as well as correct phone numbers for the WECC RC. A Settlement Agreement covering violations of CIP-001-1 R2 for SNCL was filed with FERC under NP11-130-000 on February 28, 2011. On March 25, 2011, FERC issued an order stating it would not engage in further review of the Notice of Penalty. WECC determined that the instant issue is appropriate for FFT treatment because in this instance, although SNCL's reporting procedures did not contain the correct email address for the RC, SNCL's electric control center still maintained current contact information for appropriate parties in the Interconnection as well as correct phone numbers for the WECC RC.	To mitigate this issue, SNCL updated its sabotage reporting procedure with the correct information. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Avista Corporation (AVA)	NCR05020	WECC2013012062	FAC-501-WECC-1	R3	On March 1, 2013, AVA submitted a Self-Certification to WECC stating that, as a Transmission Owner, it had an issue with FAC-501-WECC-1 R3. AVA reported that it had an established Transmission Maintenance and Inspection Plan (TMIP) that required it to perform biennial infrared inspection on its circuit breakers. AVA reported that it failed to conduct one of its biennial infrared inspections at its W-5482 Walla Walla circuit breaker located in the Grant County PUD's Wanapum 230 kV switching station. AVA reported that its failure to conduct the biennial infrared inspection resulted in an issue with FAC-501-WECC-1 R3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. This issue included only 1 out of 88 (1.14%) circuit breakers included in AVA's TMIP. Additionally, the circuit breakers are continuously monitored and have alarms attached if a triggering event occurs.	To mitigate this issue, AVA completed the required biennial infrared testing on its W-5482 circuit breaker.
Western Electricity Coordinating Council (WECC)	Simpson Tacoma Kraft Co., LLC (STK)	NCR10303	WECC2013012191	VAR-002-1.1b	R1	On April 5, 2013, STK submitted a Self-Report to WECC stating that, as a Generator Operator and Generator Owner, it had an issue with VAR-002-1.1b R1. Specifically, STK reported that the STK Biomass Cogen unit was taken offline on March 19, 2013 at 12:10 p.m. to replace turbine generator communication cards on the turbine control system. Before taking the generator offline, STK disabled the automatic voltage regulator's (AVR's) power factor mode. On March 19, 2013 at 5:55 p.m., the generator work was completed and the unit came back online. When the unit was resynchronized to the system, the replacement cards caused the unit to synchronize in the power factor mode of operation instead of the required AVR control mode. The incorrect mode of operation was not discovered until 11:30 a.m. on March 20, 2013, at which time STK immediately changed the voltage control from power factor mode to AVR control mode and notified the Transmission Operator (TOP).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. STK's single biomass generator operated in the power factor mode for 17 hours and 35 minutes without STK notifying its TOP. This generator is a steam turbine unit with a name plate rating of 55 MW. Further, at the time the AVR was in power factor mode, STK had a power system stabilizer (PSS) in service that would automatically deliver additional voltage support if needed. As a result, the voltage schedule with the TOP was always maintained. A Settlement Agreement covering a violation of VAR-002-1.1a R1 for STK was filed with FERC under NP12-40-000 on July 31, 2012. On August 30, 2012, FERC issued an order stating it would not engage in further review of the Notice of Penalty. WECC determined that the instant issue is appropriate for FFT treatment. Previously, WECC determined STK operated its generation unit in the Power Factor mode for a period of two Years. This was a result of the engineering design for the unit did not allow or provide for the use of the AVR in the AVR control mode. WECC determined that this instance of noncompliance is different then the violation addressed herein, because the first instance was due to the capability of the generator controls whereas this issue is a result of human error. For these reasons, WECC considers STK's compliance history as a factor in its designation of these remediated issues for FFT treatment.	To mitigate this issue, STK: 1) returned AVR to voltage control mode; 2) installed a software jumper around the internal bits to force the output signal to the AVR for power factor control mode to always be off; 3) updated the steam turbine startup process to include steps to confirm the AVR and PSS status after generator synchronization; and 4) performed operator awareness training - Immediate training to ensure all operators understand the AVR operational capabilities/requirements and display indications. WECC has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Portland General Electric Company (PGE)	NCR05325	WECC2013012223	VAR-002-1.1b	R3	On April 15, 2013, PGE submitted a Self-Report to WECC stating that, as a Generator Operator, it had an issue with VAR-002-1.1b R3. PGE reported that on two separate occasions certain power system stabilizers (PSS) were not enabled as its generators were brought online. PGE stated that the first instance occurred on March 19, 2013. PGE reported that on March 18, 2013, while undergoing an economic outage4, a technician was updating the Toolbox programming application of its Coyote Springs Unit 1 Gas Turbine (Unit 1) control system human machine interface (HMI). As part of the update, the technician rebooted Unit 1's Mark V controllers of the turbine control system and the EX2100e controllers of the generator excitation system. After the controllers were rebooted, the PSS defaulted to the "OFF" or "Not Enabled" state. When the combustion turbine generator (CTG) restarted on March 19, 2013, the PSS was in the "OFF" or "Not Enabled" status on the exciter. PGE reported that its crews discovered the status of the PSS on March 25, 2013 at 1:15 a.m. and that the crews promptly changed the PSS to automatic mode and notified its Transmission Operator (TOP). PGE reported that the second incident occurred on April 3, 2013. PGE reported that a power supply board in its Coyote Springs Unit 2 combustion turbine generator (CTG) exciter was replaced. PGE reported that when it restarted the CTG at approximately 5:00 a.m., the PSS was in the "OFF" or "Not Enabled" state. PGE reported that its crews discovered the status of the PSS at approximately 6:05 a.m. and promptly corrected the status and informed its TOP of the status change.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. PGE had several compensating measures which limited the risks associated with the issue. First, PGE has installed automatic voltage regulators (AVR) on both Unit 1 and Unit 2. The AVRs were fully functional in each occurrence and would have acted properly had any voltage fluctuations or disturbances occurred. Additionally, in each instance, PGE's other three turbines had functioning PSSs and AVRs that would also have functioned in the event of any voltage fluctuations. A Settlement Agreement covering violations of VAR-002-1.1b R3 for PGE was filed with FERC under NP13-16-000 on December 31, 2012. On January 30, 2013, FERC issued an order stating it would not engage in further review of the Notice of Penalty. WECC determined that the instant issue is appropriate for FFT treatment because the current issue relates to PGE's PSS devices. Each of the Units involved received some type of maintenance and upon restart the PSSs failed to operate as expected.	To mitigate this issue, PGE: 1) changed the PSS attached to Unit 1 from "Not Enabled" to "Enabled" informed its TOP of the status change; and 2) changed the PSS attached to Unit 2 from "Not Enabled to "Enabled" and informed its TOP of the status change.

Attachment A-2

June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2012009680	CIP-007-1	R2; R2.1	During an on-site Compliance Audit, FRCC determined that FRCC_URE1 had an issue with CIP-007-1 R2.1. FRCC_URE1 could not provide evidence to demonstrate that only ports required for normal and emergency operations were enabled for all of its Critical Cyber Assets. For the identified Cyber Assets, scans demonstrated that one port was open which was not documented as a port required for normal and emergency operations. Although a different port was documented in the list of authorized ports for the Cyber Assets, vendor documentation did not support the need for this port and it would vary each time the application was restarted.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk was reduced because the open port varied each time the application was restarted, requiring a new port scan on the system to find the port. The Cyber Asset is located within an Electronic Security Perimeter (ESP) and Physical Security Perimeter. Furthermore, access to the range of unauthorized open ports is closed at the ESP access point firewall preventing access to the Cyber Asset from outside the ESP.	To mitigate this issue, FRCC_URE1: 1) updated its authorized ports and services by asset class - application servers document, to remove the unneeded port and associated service from the list of authorized ports and services; 2) submitted a technical feasibility exception (TFE) to document implementation of the windows firewall to block the unauthorized ports that are not required for operation and cannot be disabled by the vendor supplied application; and 3) verified the TFE mitigating and compensating protections are only allowing the authorized services to listen for connections on authorized ports. FRCC has verified the completion of all mitigation activity.
Florida Reliability Coordinating Council (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2013011736	CIP-005-3a	R3; R3.2	FRCC_URE1 self-reported that it had an issue with CIP-005-3a R3.2. For approximately one minute, FRCC_URE1's backup logging monitoring and alerting Cyber Asset was unable to detect and alert for attempts at or actual unauthorized accesses when it had to switch from the primary to backup monitoring Cyber Asset during a scheduled maintenance update of the primary logging Cyber Asset. FRCC_URE1 did not timely submit a Technical Feasibility Exception (TFE) for the Cyber Asset. It did, however, have a manual process in place to detect and alert for attempts at or actual unauthorized accesses although not clearly documented.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was reduced because FRCC_URE1 had a manual procedure (although not clearly documented) in place for the backup monitoring and logging Cyber Asset to detect and alert (manually) for attempts at or unauthorized accesses. Furthermore, the duration of the issue was short, one minute, and the issue was a result of an administrative oversight in not submitting the TFE.	To mitigate this issue, FRCC_URE1: 1) submitted a TFE for the Cyber Asset's inability to detect and alert; and 2) updated documentation to sufficiently articulate manual review process. FRCC has verified the completion of all mitigation activity.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012011475	CIP-002-1	R1; R1.2.2; R1.2.3	During a Compliance Audit, MRO discovered that MRO_URE1 failed to have a risk-based assessment methodology (RBAM) which considered the following assets: 1) transmission substations that support the reliable operation of the bulk electric system (BES), in accordance with CIP-002-1 R1.2.2; and 2) generation resources that support the reliable operation of the BES, in accordance with CIP-002-1 R1.2.3. Specifically, MRO_URE1 failed to include criteria in order to determine criticality of substations below 230 kV, generators below 100 MW, and transmission and generation assets required for system restoration. Instead of developing criteria, MRO_URE1 relied upon a statement from its subject matter expert (SME). MRO_URE1 also relied upon a similar statement for generators under 100 MW. While engineering judgment is permissible in an RBAM, MRO determined that further documentation of this assertion was necessary. Furthermore, during mitigation, MRO discovered that preliminary asset lists, used to exercise the RBAM, had some discrepancies. However, those discrepancies were found to be assets which were not owned by MRO_URE1, and were erroneously included in its asset list.	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 MRO_URE1's documentation was insufficient for its justification of excluding these assets from its assessment, MRO_URE1 asserted that its SMEs have sufficient engineering experience with other system studies in this area to make such determinations. MRO_URE1 failed to properly document its SME experience which qualified them to make such determinations. Additionally, the documentation issue with the preliminary asset lists did not impact MRO_URE1's overall Critical Asset list. The revisions did not result in any additions to MRO_URE1's actual list of Critical Assets. Therefore, MRO determined that this issue posed a minimal risk to the BPS.	To mitigate this issue, MRO_URE1 revised its RBAM to include more detail regarding the engineering assessment process to achieve the following: 1) clarify the criteria for including or excluding BPS assets from further detailed analysis during the application of the RBAM; 2) provide additional documentation specific to the assessment of restoration resources; and 3) clarify the assessment method for assets that are owned by other registered entities but operated by MRO_URE1.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2) Southern Minnesota Municipal Power Agency (SMMPA)	NCRXXXXX	MRO2012010128	CIP-002-1	R1	During a Compliance Audit, MRO discovered that MRO_URE2 failed to adequately document evaluation criteria used to assess its Critical Assets to determine the impact on the Bulk Electric System (BES). CIP-002-1 R.1.1 requires the Responsible Entity to maintain documentation describing its risk-based assessment methodology (RBAM) that includes procedures and evaluation criteria. MRO_URE2 included its procedures used to categorize assets in its RBAM, but did not include evaluation criteria. MRO_URE2's RBAM contained impacts to the BES that were conclusory and did not identify how its conclusions were derived for classifying its Critical Assets. For example, MRO_URE2's control center was identified as having a low probability of an event and minimal impact on the BES, but did not state how those conclusions were determined.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). MRO_URE2 does not operate generation or transmission facilities. As a result, its control center is used as a "view-only" tool. Although MRO_URE2 did not include evaluation criteria in its RBAM, MRO_URE2's previous determination regarding its list of Critical Assets remained the same after MRO_URE2 clarified its evaluation criteria.	To mitigate this issue, MRO_URE2 updated its RBAM pursuant to CIP-002 R1, which incorporated bright-line criteria from new CIP versions. Under its current RBAM, MRO_URE2's list of Critical Assets remains the same.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3) City Of Grand Island, NE (GRIS)	NCRXXXXX	MRO2012010160	CIP-002-1	R1; R1.1	During a Compliance Audit, MRO discovered that MRO_URE3 failed to maintain documentation describing its risk-based assessment methodology (RBAM) that includes procedures and evaluation criteria, in accordance with CIP-002-1 R1.1. MRO_URE3 used a formula for determining criticality. Although MRO_URE3 assigned numbers for both of these scales for each asset, it failed to document how the scale entries were obtained.	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 MRO_URE3's RBAM lacked clear documentation in the use of the evaluation criteria for determining criticality, MRO_URE3 does not have any Critical Assets. Additionally, MRO_URE3 is a small entity with limited possible impact on the BPS.	To mitigate the issue, MRO_URE3 documented how each rating scale number is determined and how assets fit each rating. MRO has verified the completion of all mitigation activity.

Attachment A-2
June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012125	CIP-005-3a	R5; R5.2	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-005-3a R5.2. RFC_URE1 changed the way it monitors and logs access at access points to its Electronic Security Perimeters (ESPs) when it replaced a RFC_URE1-owned and managed monitoring and logging appliance with a third-party monitoring and logging service. However, RFC_URE1 failed to update the documentation reflecting the modification of the network and controls within 90 calendar days of this change. RFC_URE1's failure to update documentation following its implementation of a new monitoring and logging service also resulted in RFC_URE1's noncompliance with Reliability Standard CIP-008-3 R1, as described in issue RFC2013012131.	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 issue was a documentation deficiency related to its reference of a previous version of its monitoring and logging service, rather than the new monitoring and logging service within its CIP-005-3 documentation. RFC_URE1 did not leave its devices unprotected as a result of this documentation error. Rather, in implementing the change from one system to another system, RFC_URE1 did not deactivate its previous monitoring and logging appliance until the new monitoring and logging service was up and running, in order to ensure that there was no interruption in ESP monitoring and logging. In addition, RFC_URE1 personnel responsible for ESP monitoring and logging were directly involved in the transition from the previous monitoring and logging appliance to the new monitoring and logging service, and were therefore familiar with the changes to the monitoring infrastructure. Furthermore, the relevant personnel were continuously able to receive alerts and event data and were knowledgeable about how to customize alerts and access and review log files both during and after the transition to the new monitoring and logging service. The issue was a clerical error that had no impact on its operational capability and which did not interrupt its monitoring or logging of the ESP.	To mitigate this issue, RFC_URE1 modified its change ticket templates for its CIP-003 change control and configuration management process to require change submitter to determine whether, in each instance, RFC_URE1 should update additional documents that might be affected by a change.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012129	CIP-007-1	R4	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-007-1 R4 because it submitted its technical feasibility exception (TFE) request for its monitoring services late due to vendor delays in providing RFC_URE1 the required information. Additionally, RFC_URE1 overlooked the need to file TFEs for two switches, due to the operational functionality of these devices. For all three devices, RFC_URE1 was unable to install anti-virus software and malware prevention tools, but failed to document the compensating measures applied to mitigate risk exposure or acceptance of risk.	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 provided alternate controls to protect its systems from cybersecurity breaches where anti-virus software and malware prevention tools were technically infeasible. Each implicated system and device is located behind a Physical Security Perimeter (PSP). Additionally, the two switches are located inside an Electronic Security Perimeter (ESP) and utilize a rudimentary proprietary operating system that utilizes magnetic relays to switch between routers and that is not capable of anti-virus or malware installation. RFC_URE1 follows its malware prevention program for all other devices. Furthermore, RFC_URE1 has not experienced any incidents or security breaches during the time frame of this issue.	To mitigate this issue, RFC_URE1 implemented the compensating measures, which included all equipment being inside a six-wall PSP and the switches within the ESP, described in its TFE Part B submittals to mitigate risk exposure.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010394	CIP-007-1	R5; R5.3.2	RFC_URE1 submitted a Self-Certification and approximately a week later RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-007-1 R5. RFC_URE1 failed to timely notify Reliability*First* of instances related to its operating system where, due to technical infeasibility, RFC_URE1 did not require the use of passwords consisting of a combination of alpha, numeric, and "special" characters.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although RFC_URE1 does not have technical controls regulating password complexity for its operating system, RFC_URE1 had procedural controls in place which require all system users to utilize CIP compliant passwords where possible. RFC_URE1 also submits email reminders to all system users regarding the proper password complexity. RFC_URE1 utilized technical controls to enforce the password complexity to the maximum extent capable by the operating system, which includes, at a minimum, a forced password character length of at least eight characters. Additionally, the equipment that is running the operating system is inside a Physical Security Perimeter and an Electronic Security Perimeter which RFC_URE1 monitors 24 hours a day, seven days a week.	To mitigate this issue, RFC_URE1 submitted a Technical Feasibility Exception to Reliability*First* and reminded operators of the CIP-007 R5.3.2 password complexity requirements.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012130	CIP-007-1	R6	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-007-1 R6. For two Cyber Assets within the Electronic Security Perimeter, namely two switches, RFC_URE1 did not ensure that these devices implement automated tools or organizational process controls to monitor system events related to cybersecurity, nor did RFC_URE1 submit a Technical Feasibility Exception (TFE) with Reliability*First* to document the technical infeasibility of implementing such controls.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The limited operational functionality of the two switches protects RFC_URE1's system from cybersecurity breaches, since the devices are used only to switch incoming Supervisory Control and Data Acquisition (SCADA) data feeds between a redundant pair of front-end processors. A SCADA and energy management system (EMS) server controls the operation of both switches and will command an "A to B" or "B to A" switchover if it detects a loss of incoming SCADA data. The SCADA/EMS server's detection of data loss effectively compensates for the fact that the switches themselves have no monitoring capabilities. Furthermore, the SCADA/EMS server has been given the protections as applicable from CIP-002 through CIP-009. Therefore, RFC_URE1 implemented measures to provide protection to its system from cybersecurity events.	To mitigate this issue, RFC_URE1: 1) filed a TFE with Reliability*First* related to the switches; and 2) modified its change ticket templates used for CIP-003 change control and configuration management to require change submitters to determine whether one or more TFEs will be required for any new Cyber Asset subject to CIP requirements. If TFE(s) are required, the submitter will be required to enter Reliability*First* -assigned TFE identifier(s) before change ticket can be closed out.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012010395	CIP-007-3	R9	RFC_URE1 submitted a Self-Certification to Reliability*First* stating that it had an issue with CIP-007-3 R9. RFC_URE1 failed to annually review and update all documentation specified in Standard CIP-007-3. Specifically, RFC_URE1 failed to annually review and update the following CIP-007-3 documentation in 2011: 1) system security management: ports and services procedures; 2) system security management: security patch management; 3) system security management: malicious software prevention; 4) system security management: Cyber Asset disposal or redeployment procedures; and 5) system security management: cyber vulnerability assessments. Instead, within RFC_URE1's document management system, RFC_URE1 mislabeled the document review frequency label by inserting an incorrect document review due date and thereafter failed to annually review all CIP-007-3 documentation.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue was caused by a data entry mistake and was corrected within five months. Only minor updates to the subject document were necessary. Finally, RFC_URE1 performed the necessary reviews and updates for 2012. .	To mitigate this issue, RFC_URE1: 1) labeled documents correctly in its document management system in order to ensure that it conducts future document reviews on an annual basis; 2) created a tool to track document review dates; and 3) reviewed its documentation and added those documents that it had previously not reviewed on an annual basis to its review matrix. Reliability*First* has verified the completion of all mitigation activity.

Attachment A-2
June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012131	CIP-008-3	R1; R1.4	RFC_URE1 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-008-3 R1.4. RFC_URE1 changed its system for generating automated Cyber Security Incident alerts, but failed to update its Cyber Security Incident response plan within 30 calendar days of this change. RFC_URE1's failure to update documentation following its implementation of a new monitoring and logging service also resulted in RFC_URE1's noncompliance with Reliability Standard CIP-005-3a R5.2, as described in RFC2013012125.	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 issue was a documentation deficiency related to its reference of a previous version of its monitoring and logging service, rather than the new monitoring and logging service within its Cyber Security Incident response plan. RFC_URE1 did not leave its devices unprotected as a result of this documentation error. Rather, in implementing the change from one system to another system, RFC_URE1 did not deactivate its previous monitoring and logging appliance until the new monitoring and logging service was up and running, in order to ensure that there was no interruption in Electronic Security Perimeter (ESP) monitoring and logging. In addition, RFC_URE1 personnel responsible for (ESP) monitoring and logging were directly involved in the transition from the previous monitoring and logging appliance to the new monitoring and logging service, and were therefore familiar with the changes to the monitoring infrastructure. Furthermore, the relevant personnel were continuously able to receive alerts and event data and were knowledgeable about how to customize alerts and access and review log files both during and after the transition to the new monitoring and logging service. The issue was a clerical error that had no impact on its operational capability and which did not interrupt its monitoring or logging of the ESP.	To mitigate this issue, RFC_URE1: 1) updated its Cyber Security Incident response plan; and 2) modified its change ticket templates for its CIP-003 change control and configuration management process to require change submitter to determine whether, in each instance, should update additional documents that might be affected by a change.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2013012132	CIP-009-3	R1	RFC_URE1 submitted a Self-Report to Reliability*First* stating that had an issue with CIP-009-3 R1. RFC_URE1 failed to annually review two documents: 1) the RFC_URE1 IT plan dealing with backup and recovery; and 2) the site replication and failover plan, which are incorporated by reference into RFC_URE1's recovery plan.	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 conducted an annual review on the remainder of the recovery plan, except the two documents which were incorporated by reference. Additionally, RFC_URE1 determined that the two referenced documents that were not reviewed on an annual basis did not require any updates.	To mitigate this issue, RFC_URE1 added the two missed documents to its annual review matrix and reviewed each document.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2) Dearborn Industrial Generation, L.L.C. (Dearborn)	NCRXXXXX	RFC2013012302	CIP-003-1	R2; R2.1	RFC_URE2 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-003-1 R2. RFC_URE2 could not locate a separate specific document that identified the senior manager by name, title, and date of designation for approximately 28 months. However, the senior manager who approved and signed the CIP-related documents, including the Critical Asset assessment and subsequent lists of Critical Assets and Critical Cyber Assets (CCAs) was the appropriate senior manager during that time period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). This was a documentation issue only. The senior manager that approved and signed the CIP-related documents was the appropriate senior manager during that time period and is now retired. RFC_URE2 has no Critical Assets or CCAs, reducing the likelihood that this issue would cause a risk to the reliability of the BPS.	To mitigate this issue, RFC_URE2: 1) conducted a review of its CIP procedure; 2) revised its designation of senior manager letter and stored it in the electronic document management program for document retention. In addition, the electronic data tracking system will generate an annual reminder to review senior manager assignments; and 3) created a managerial transition checklist as a reminder to validate the senior manager assignment within 30 days of senior manager assignment.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2013012420	CIP-003-2	R1	Reliability*First* conducted a Compliance Audit and determined that RFC_URE3 had an issue with CIP-003-2 R1. RFC_URE3 failed to ensure that its cybersecurity policy addresses all of the requirements in Standards CIP-002 through CIP-009.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. RFC_URE3's policy generally addressed the NERC CIP Standards, even though it did not specifically address each Requirement. RFC_URE3 implemented its cybersecurity policy with limited deficiencies not attributed to the policy document.	To mitigate this issue, RFC_URE3 revised its cybersecurity policy to address the requirements of Standards CIP-002 through CIP-009.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012012427	CIP-005-1	R4; R4.2, R4.3, R4.4	Reliability*First* conducted a Compliance Audit. Reliability*First* identified that RFC_URE3 had an issue with CIP-005-1 R4. RFC_URE3's cyber vulnerability assessment (CVA) of electronic access points did not identify all access points, such as WAN routers and gas server room modems. As a result, RFC_URE3 failed to conduct a complete review that only ports and services required for operations at access points are enabled (R4.2) and failed to discover all access points to the Electronic Security Perimeter (R4.3). RFC_URE3 conducts an automatic and a manual review of controls for default accounts, passwords, and network management community strings but, in its CVA failed to include the gas server room modems in the manual review (R4.4).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. RFC_URE3 performed CVAs for its electronic access points, although it did not document the consideration of R4.2, R4.3, and R4.4. In addition, for the access points that RFC_URE3 did not discover, RFC_URE3 classified the access points it failed to discover as Critical Cyber Assets (CCAs) and afforded them the protective measures of CCAs.	To mitigate this issue, RFC_URE3 revised its documented process for CVAs of access points to the Electronic Security Perimeter.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2013012428	CIP-006-1	R1	Reliability*First* conducted a Compliance Audit. Reliability*First* identified that RFC_URE3 had an issue with CIP-006-1 R.1. Reliability*First* discovered an Electronic Security Perimeter cable that extended outside the Physical Security Perimeter (PSP). In addition, Reliability*First* discovered that RFC_URE3 failed to identify an emergency exit door as an access point on its PSP drawing.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The cabling is located under a raised floor for a short distance on the floor of the corporate office, which has limited access. The door at issue is an emergency exit only and it is incapable of opening from the outside. If opened from the inside, an alarm activates and security would respond to the alarm. In addition, the door is located inside a building with limited access.	To mitigate this issue, RFC_URE3 installed conduit around the cable at issue and added the emergency exit door to the PSP drawing.

Attachment A-2

June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
ReliabilityFirst Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2013011665	CIP-006-3c	R1	RFC_URE4 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-006-3c R1. RFC_URE4 decommissioned a Physical Security Perimeter (PSP) at a power plant because it moved two workstations into another PSP at the plant. RFC_URE4 performed a routine physical walk-down of the power plant to validate network documentation. During the walk-down, RFC_URE4 discovered that two Cyber Assets in the decommissioned PSP, one critical and one non-critical, remained connected to the Electronic Security Perimeter (ESP) through the power plant's main site distribution switch (which was located in an active and protected PSP. As a result, two Cyber Assets remained connected to ESP after RFC_URE4 decommissioned the PSP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The devices at issue still had the protections of the ESP. In addition to the protections of the ESP, these devices utilize a non-Windows based operating system that is not as susceptible to mainstream viruses. Although lack of physical protection presents an increased risk of access, the decommissioned PSP was wholly contained on a site with restricted access and perimeter security protection, reducing the likelihood of unauthorized access.	To mitigate this issue, RFC_URE4 removed the devices from the ESP and revised its current change control process to ensure it all business units understand the process of decommissioning PSPs. Reliability*First* has verified the completion of all mitigation activity.
ReliabilityFirst Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2013011946	CIP-005-1	R1; R1.4	RFC_URE4 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-005-1 R1. During a physical walk-down of all CIP Physical Security Perimeters (PSPs), RFC_URE4 discovered an undocumented switch residing in the Electronic Security Perimeter (ESP) and PSP at a power plant. The switch was acting as a hub to connect one of RFC_URE4's paperless chart recorders to a different switch. RFC_URE4 failed to identify and protect this switch as required by CIP-005-3a R1.4. RFC_URE4 removed the switch from the ESP. RFC_URE4 submitted another Self-Report to Reliability*First* identifying an additional issue with CIP-005-1 R1.4, consolidated into RFC2013011946. During its annual physical and electronic walk down of the power plant, RFC_URE4 discovered two undocumented non-critical Cyber Assets within the ESP. The devices, a wireless gateway device and a signal converter, were connected to a router in the plant's ESP. RFC_URE4 failed to identify these devices as required by CIP-005-1 R1.4. RFC_URE4 disconnected the wireless gateway device from the router and RFC_URE4 disconnected the signal converter from the router.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Regarding the undocumented switch, the switch utilized a non-Windows operating system that is not as susceptible to mainstream viruses. The switch resided in a PSP and the paperless chart recorder was the only device to which it was connected. Both the wireless gateway device and the signal converter device were located within an ESP and PSP. Regarding the wireless gateway device, RFC_URE4 never configured it with an IP address and it was therefore unable to communicate or be discovered on the network. In addition, wireless transmission on the device was inactive. Regarding the signal converter, RFC_URE4 utilizes the device to remotely monitor data on the generating unit, which does not affect plant operation. In addition, its monitoring capability was redundant because a primary means of monitoring the asset was in place. As a result, it was less likely that unauthorized access to Critical Cyber Assets could occur through these devices.	To mitigate this issue, RFC_URE4: 1) removed the device from the ESP and PSP; and 2) removed the devices after verifying that their removal would not impact the reliability of the system.
ReliabilityFirst Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2013012068	CIP-004-4	R2	RFC_URE4 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-004-4 R2. RFC_URE4 added a new contractor to the network engineering security group to enable the contractor to access a non-NERC system. This contractor did not have cybersecurity training. Adding the contractor to this group inadvertently provided the contractor with cyber access to certain routers and switches, which are Critical Cyber Assets (CCAs). During a periodic user access review, RFC_URE4 discovered this access and immediately revoked it. RFC_URE4 submitted a Self-Report to Reliability*First* identifying an additional issue with CIP-004-4, consolidated into RFC2013012068. As part of an internal effort to improve its reporting mechanism for physical and electronic access, RFC_URE4 discovered two contract employees and one RFC_URE4 employee that had not completed annual training but retained physical access to one or more Physical Security Perimeters. RFC_URE4's internal policy requires employees and contractors to renew their annual training once per calendar year, not to exceed 15 months. In each instance, the employee and the supervisor of the employee were notified that the training was set to expire. Upon discovery, RFC_URE4 revoked access for all three individuals.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Regarding the failure to conduct cybersecurity training prior to granting access, the contractor had a current and valid personnel risk assessment (PRA). In addition, when RFC_URE4 reviewed the logs, it determined that the contractor did not access any of the CCAs. It is unlikely that the contractor would have known about the access to such devices as the contractor's job roles did not include accessing NERC CIP routers or switches. Regarding the failure to complete annual cybersecurity training, the individuals had physical access only, and all three individuals had current and valid PRAs. All three individuals had completed cybersecurity training prior to being granted access.	To mitigate this issue, RFC_URE4: 1) revoked the employees' access, and implemented a system-generated nightly list of all personnel with electronic and physical access that have qualifications in jeopardy of surpassing the allotted annual review period. This list will be automatically distributed to the NERC compliance organization for review and monitoring; and 2) communicated the importance of timely access revocation to all RFC_URE4 leaders.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2013012099	CIP-006-3c	R1; R1.6	RFC_URE5 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-006-3c R1.6. RFC_URE5 did not log the exit and re-entry of five visitors to a physical security perimeter (PSP). Specifically, RFC_URE5 escorted the five visitors from a conference room inside a PSP to a lab area outside the PSP, but within the same facility, to participate in a demonstration. RFC_URE5 then escorted the five visitors back into the PSP to gather equipment, and then escorted them back out of the PSP to participate in the demonstration. At the close of the demonstration, RFC_URE5 escorted the five visitors back to the PSP. When escorting the visitors into and out of the PSP, RFC_URE5 neglected to log the visitors' exit and re-entry into the PSP pursuant to CIP-006-3c R1.6.1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The five visitors had an escort for the duration of the issue. Additionally, the RFC_URE5 escort had successfully completed CIP training, had a valid personnel risk assessment and was authorized to have unescorted access to the PSP at issue. Finally, RFC_URE5 logged initial entry and final exit from the PSP of the five individuals, just not the exit and re-entry associated with the lab demonstration.	To mitigate this issue, RFC_URE5: 1) discussed the incident with the CIP escort and reinforced proper logging procedures; and 2) provided all department personnel with re-education on CIP escort responsibilities during a-department meeting.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2013012098	CIP-004-1	R4	RFC_URE5 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-004-1 R4. RFC_URE5 discovered that an authentication source was configured to grant a non-CIP directory service group access to Critical Cyber Assets (CCAs). However, RFC_URE5 had not authorized cyber access to two members of the group through its regulatory access authorization database system.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Both members of the group who lacked cyber authorization from RFC_URE5 had valid CIP training and personnel risk assessments for the duration of the issue. The issue with CIP-004-1 R4 did not provide non-CIP personnel with CIP access; rather it provided cyber access to two CIP-qualified individuals without first formally authorizing access. Finally, the two individuals at issue were unaware they had cyber access to the CCAs at issue and at no time attempted to access the CCAs.	To mitigate this issue, RFC_URE5: 1) removed the two individuals from the group; 2) disabled the group's ability to access CCAs; 3) created and implemented new naming conventions to delineate between CIP and non-CIP directory service groups, reducing the likelihood that RFC_URE5 will inadvertently assign a non-CIP directory service group to a CIP-controlled access list; and 4) reviewed all directory service groups for similar situations and did not discover any
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2013012100	CIP-006-3c	R5	RFC_URE5 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-006-3c R5. During a five-day period, RFC_URE5 did not continuously monitor an access point into a physical security perimeter (PSP) with an alarm system or human observation. RFC_URE5 initially configured an access point to a PSP with a portal mantrap and an exterior steel door with a keypad connected to its Physical Access Control System. During a renovation of the access point RFC_URE5 removed the mantrap and with it the alarm for unauthorized access. During this renovation, RFC_URE5 monitored for unauthorized access with human observation 24 hours a day, seven days a week from an office located next to the access point. However, when FE Utilities renovated that office, it relocated the individuals observing the access point for five days. The employee who decided to relocate the individuals from the office for five days incorrectly believed an alarm input was installed on the exterior steel door adjacent to the keypad. RFC_URE5 failed to monitor the access point with an alarm system or human observation during that five-day period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Access to the PSP was controlled and logged by an exterior steel door with the keypad access system for the duration of the issue. Additionally, access to the building in which the PSP is located was continuously monitored by a guard staff stationed 24 hours a day, seven days a week for the duration of the issue.	To mitigate this issue, RFC_URE5 installed an alarm on the access point of the PSP.

Attachment A-2

June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC2013012193	CIP-004-1	R4	RFC_URE6 submitted a Self-Report to Reliability*First* stating that it had an issue with CIP-004-1 R4. RFC_URE6 discovered that an authentication source was configured to grant a non-CIP directory service group -access to Critical Cyber Assets (CCAs). However, RFC_URE6 had not authorized cyber access to two members of the group through its regulatory access authorization database system.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Both members of the group who lacked cyber authorization from RFC_URE6 had valid CIP training and personnel risk assessments for the duration of the issue. The issue with CIP-004-1 R4 did not provide non-CIP personnel with CIP access; rather it provided cyber access to two CIP-qualified individuals without first formally authorizing access. Finally, the two individuals at issue were unaware they had cyber access to the CCAs at issue and at no time attempted to access the CCAs.	To mitigate this issue, RFC_URE6: 1) removed the two individuals from the group; 2) disabled the group's ability to access CCAs; 3) created and implemented new naming conventions to delineate between CIP and non-CIP directory service groups, reducing the likelihood that RFC_URE6 will inadvertently assign a non-CIP directory service group to a CIP-controlled access list; and 4) reviewed all directory service groups for similar situations and did not discover any additional instances of possible noncompliance.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC2012010380	CIP-008-3	R1	RFC_URE7 self-certified to Reliability*First* that it had an issue with CIP-008-3 R1. While RFC_URE7 had a procedure for updating their Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE7 did not update its Cyber Response Plans within 30 calendar days on four separate occasions. Specifically, RFC_URE7 failed to change referenced procedure versions or designation numbers in its Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE7 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE7: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated its Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE7 removed unnecessary document references within the Cyber Response Plan, reducing any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE7 to update the Cyber Response Plan following minor changes to referenced documents.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 8 (RFC_URE8)	NCRXXXXX	RFC2012010381	CIP-008-3	R1	RFC_URE8 self-certified to Reliability*First* that it had an issue with CIP-008-3 R1. While RFC_URE8 had a procedure for updating their Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE8 did not update its Cyber Response Plans within 30 calendar days on four separate occasions. Specifically, RFC_URE8 failed to change referenced procedure versions or designation numbers in its Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE8 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE8: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated its Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE8 removed unnecessary document references within the Cyber Response Plan, reducing any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE8 to update the Cyber Response Plan following minor changes to referenced documents.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 9 (RFC_URE9)	NCRXXXXX	RFC2012010382	CIP-008-3	R1	RFC_URE9 self-certified to Reliability*First* that it had an issue with CIP-008-3 R1. While RFC_URE9 had a procedure for updating their Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE9 did not update its Cyber Response Plans within 30 calendar days on four separate occasions. Specifically, RFC_URE9 failed to change referenced procedure versions or designation numbers in its Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE9 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE9: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated its Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE9 removed unnecessary document references within the Cyber Response Plan, reducing any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE9 to update the Cyber Response Plan following minor changes to referenced documents.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 10 (RFC_URE10)	NCRXXXXX	RFC2012010383	CIP-008-3	R1	RFC_URE10 self-certified to Reliability*First* that it had an issue with CIP-008-3 R1. While RFC_URE10 had a procedure for updating their Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE10 did not update its Cyber Response Plans within 30 calendar days on four separate occasions. Specifically, RFC_URE10 failed to change referenced procedure versions or designation numbers in its Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE10 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE10: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated its Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE10 removed unnecessary document references within the Cyber Response Plan, reducing any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE10 to update the Cyber Response Plan following minor changes to referenced documents.

Attachment A-2
June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 11 (RFC_URE11)	NCRXXXXX	RFC2012010384	CIP-008-3	R1	RFC_URE11 self-certified to ReliabilityFirst that it had an issue with CIP-008-3 R1. While RFC_URE11 had a procedure for updating their Cyber Response Plans within 30 calendar days of any changes, it did not consistently implement that procedure. RFC_URE11 did not update its Cyber Response Plans within 30 calendar days on four separate occasions. Specifically, RFC_URE11 failed to change referenced procedure versions or designation numbers in its Cyber Response Plans and did not update the Standard and Requirement language within 30 calendar days of the change from version 2 to version 3 of the CIP Reliability Standards.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The issue is a documentation issue. The changes RFC_URE11 failed to update within 30 calendar days included changing referenced procedure versions or designation numbers and the Standard and Requirement wording arising from the transition from version 2 of the CIP Standards to version 3. Additionally, the changes were administrative in nature, rather than substantive changes to the Cyber Response Plan.	To mitigate this issue, RFC_URE11: 1) consolidated several independent procedures that made up its Cyber Response Plan into one Cyber Response Plan. This new Cyber Response Plan corrected any deficient documentation references as well as eliminated the administrative burden of ensuring several Cyber Response Plans were updated to reflect administrative changes to referenced documents; and 2) consolidated its Cyber Response Plan with that of another registered entity following a merger. During the consolidation, RFC_URE11 removed unnecessary document references within the Cyber Response Plan, reducing any future CIP-008-3 R1.4 issues by eliminating the need for RFC_URE11 to update the Cyber Response Plan following minor changes to referenced documents.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 12 (RFC_URE12) LSP University Park, LLC (LSP University Park)	NCRXXXXX	RFC2012011286	CIP-001-1a	R2	During a Compliance Audit, ReliabilityFirst discovered that RFC_URE12 had an issue with CIP-001-1a R2. RFC_URE12 failed to have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. RFC_URE12 provided a safety manual procedure for emergency response, but the document's emergency contact list did not include appropriate contacts for the Interconnection.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that RFC_URE12 had a procedure in place for responding to suspected or actual sabotage events, including a list of contacts for reporting such events, although this list did not include appropriate parties in the Interconnection. The contact list contained names of various people within the RFC_URE12 organization, county sheriff, Federal Bureau of Investigation, local hospital, gas pipeline contacts, environmental agencies, and other state and federal contacts.	To mitigate this issue, RFC_URE12 updated its safety manual procedure to include telephone numbers for contacting the appropriate parties in the Interconnection concerning sabotage events.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 12 (RFC_URE12) LSP University Park, LLC (LSP University Park)	NCRXXXXX	RFC2012011287	CIP-001-1a	R3	During a Compliance Audit, ReliabilityFirst discovered that RFC_URE12 had an issue with CIP-001-1a R3. Although RFC_URE12 had sabotage response guidelines on file, RFC_URE12 could not provide evidence that changes to the guidelines were made available to operating personnel.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that RFC_URE12 had developed a sabotage response guidelines. In addition, RFC_URE12 held meetings, during which possible sabotage incidents may be discussed, indicating some awareness of these guidelines by personnel.	To mitigate this issue, RFC_URE12 trained plant personnel on changes to its sabotage response procedure, including changes to the contact list for reporting sabotage events.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 13(RFC_URE13)	NCRXXXXX	RFC2012010914	CIP-006-3c	R2; R2.2	RFC_URE13 submitted a Self-Report stating it had an issue with CIP-006-3c R2 to ReliabilityFirst. RFC_URE13 granted a contractor authorized cyber access to a Cyber Asset that authorizes and/or logs access to the Physical Security Perimeter (PSP) so that that contractor could restart the system if it froze and required restarting. The access did not include anything beyond restarting the system. RFC_URE13; however, failed to conduct a personnel risk assessment (PRA) for the contractor prior to granting access, as required by CIP-004-3 R3. RFC_URE13 discovered this issue within seven days of granting access and removed access that day. RFC_URE13 submitted a Self-Report to ReliabilityFirst identifying an additional occurrence of an issue with CIP-006-3c R2 related to CIP-004-3 R3. RFC_URE13 granted three contractors authorized cyber access to its physical access control system, which constitutes a Cyber Asset that authorizes and/or logs access to the PSP. RFC_URE13; however, failed to conduct a PRA for the contractors prior to granting access, as required by CIP-004-3 R3. RFC_URE13 discovered this issue within four days of granting access and removed access that day.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Regarding both occurrences, RFC_URE13's internal controls enabled RFC_URE13 to discover and remediate the issues quickly. Regarding the first occurrence, the first contractor only had access to restart the device and could not perform other functions. Had the contractor restarted the device, logging and monitoring would have remained intact. Regarding the second occurrence, the three contractors were unaware of their access rights to the physical access control system. The three contractors had access in order to support databases not related to the physical access control system. RFC_URE13 database administrators with appropriate access controlled the physical access control system and assigned work to the database administrators unrelated to the physical access control system. As a result, it was unlikely that the contractors would gain inappropriate access.	To mitigate this issue, RFC_URE13: 1) removed the restart capability from the contractor's group, remove all four contractors from that group, allow only the Cyber Security and critical infrastructure support department to access the Cyber Assets that authorize and/or log access to the PSP; and 2) continued the migration access granting to the Cyber Security and critical infrastructure support department which will process all access requests and require training and PRAs for individuals prior to granting access.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) PPG Industries, Inc. (PPG)	NCRXXXXX	SERC2013011822	CIP-003-2	R2	SERC_URE1 submitted a Self-Report to SERC stating that it had an issue with CIP-003-3 R2 because it did not document the assignment of a senior manager with overall responsibility for leading and managing implementation of, and adherence to, Standards CIP-002 through CIP-009 (CIP senior manager). SERC_URE1 had a supervisor that had assumed the responsibility of the CIP senior manager. This supervisor annually approved SERC_URE1's risk-based assessment methodology (RBAM) and resulting null lists of Critical Assets and Critical Cyber Assets (CCAs). Additionally, SERC_URE1's cybersecurity policy identified the CIP senior manager by title, but failed to identify the individual by name and the date of designation. This is the only evidence that SERC_URE1 could provide in regards to the designation of the CIP senior manager.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although SERC_URE1 did not identify its CIP senior manager by name, title, and date of designation, SERC_URE1's cybersecurity policy identified its CIP senior manager by title. The supervisor acting as SERC_URE1's CIP senior manager approved SERC_URE1's RBAM and resulting null lists for Critical Assets and CCAs. SERC_URE1 does not own or operate any Critical Assets.	To mitigate this issue, SERC_URE1: 1) revised its CIP compliance document to identify the CIP senior manager by name, title, and date of designation; 2) revised its CIP compliance document to require that any changes to the CIP senior manager must be documented within 30 calendar days of the effective date; 3) revised its CIP compliance document to allow the CIP senior manager to delegate authority for specific actions to a named delegate or delegates provided these delegations are documented in the same manner as R2.1 and R2.2, and approved by the CIP senior manager; and 4) revised its CIP compliance document to allow the CIP senior manager or delegate(s) to authorize and document any exception from the requirements of the cybersecurity policy. SERC has verified the completion of all mitigation activity.

Attachment A-2

June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCXXXXX	SPP201000446	CIP-002-1	R3; R3.3	SPP_URE1 submitted a Self-Report to SPP RE stating that it had an issue with CIP-002-1 R3.3 because it did not identify all of its Critical Cyber Assets (CCAs) associated with Critical Assets that support reliable operation of the Bulk Electric System (BES). SPP_URE1 instituted a companywide de-commissioning of all dial-up modems and routers with remote connectivity to monitoring and control devices located within its substations. Subsequently, SPP_URE1 discovered that three dial-up devices with remote connectivity to relays designated as Critical Assets were overlooked and not disabled. SPP_URE1 disabled the three devices in March 2010. The issue period was from the date the Standard became mandatory and enforceable to the date SPP_URE1 disabled the devices at 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 three dial-up devices were connected to relays for retrieving fault information only and did not control any of the associated relays. Furthermore, these devices were password-protected and located within locked control houses. Finally, the duration of the issue lasted only three months, and during that time, no events occurred that put the BPS at risk.	To mitigate the issue, SPP_URE1: 1) disabled the three dial-up devices; and 2) developed a three-step process to ensure that all CCAs associated with Critical Assets that support reliable operation to the BES are identified. SPP RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXX	TRE2012009764	CIP-003-1	R4; R4.3	During a Compliance Audit, Texas RE determined that TRE_URE1 had an issue with CIP-003-1 R4.3 because TRE_URE1 did not include within its information protection annual review process the assessment of the incidence response plan(s) as required for CIP-003-1 R4.3. Texas RE determined that the incident response plan was part of the Critical Cyber Asset (CCA) information that TRE_URE1 protected but TRE_URE1 did not perform the assessment, document the assessment results, and implement an action plan to remediate deficiencies if any, identified during an assessment of the incidence response plan. Therefore, TRE_URE1 had an issue with CIP-003-1 R4 from the date the requirement became enforceable for TRE_URE1 through the date that all mitigating activity was completed.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because TRE_URE1 stated that it performed an annual assessment of its incidence response plan. Although TRE_URE1 failed to specifically list the "incident response plan" in its annual review process document, or provide sufficient evidence of its annual assessment, TRE_URE1 stated that the incident response plan was assessed and it was protected pursuant to the rest of the protected information list.	TRE_URE1 remediated the issue with CIP-003-1 R4 by providing evidence that TRE_URE1's information protection annual review process has been updated to include the annual assessment of the incident response plan. Texas RE verified completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXX	TRE2012009768	CIP-005-1	R4; R4.4	During a Compliance Audit, Texas RE determined that TRE_URE1 had an issue with CIP-005-1 R4.4 because TRE_URE1 did not perform a complete cyber vulnerability assessment (CVA) for the electronic access points to the ESP. Specifically, TRE_URE1 failed to demonstrate that it had reviewed and implemented the network management community strings on all identified electronic access points. Therefore, TRE_URE1 had an issue with CIP-005-1 R4.4 from the date the requirement became enforceable for TRE_URE1, through the date that all mitigating activity was completed.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). The risk to reliability of the BPS was mitigated because while TRE_URE1 did not complete a review of controls for network management community strings, TRE_URE1's infrastructure is protected from penetration by various layers of protection that include: firewalls, group user authentication, shared account reviews, infrastructure reviews, employee training, cyber incidence detection, and electronic security perimeter and physical security perimeter access authentication. Texas RE determined that the instant issue is appropriate for FFT treatment because although TRE_URE1 has prior CIP violations, they were self-reported and occurred concurrently with the instant issue.	To mitigate this issue, TRE_URE1: 1) provided evidence that a complete CVA was performed; 2) offered supporting documentation; and 3) the CVA process was updated to remind the tester to retain all evidence of test results as a part of the CVA documentation. Texas RE has verified completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2) Barney M Davis	NCRXXXX Unit 1 (BMD1)	TRE2013012122	CIP-002-2	R4	On March 13, 2013, TRE_URE2 submitted a Self-Report to Texas RE, stating that it had an issue with CIP-002-2 R4. Specifically, TRE_URE2 did not have a senior manager or delegate sign its risk-based assessment methodology (RBAM), its list of Critical Assets, and its list of null Critical Cyber Assets (CCAs). TRE_URE2 designated one person as the senior manager. TRE_URE2's plant manager, instead of the designated person, signed TRE_URE2's RBAM, its list of Critical Assets, and its list of null CCAs. The plant manager had not been designated as a senior manager or delegate. TRE_URE2 designated a third person as the senior manager and the newly designated person signed and approved TRE_URE2's RBAM, its list of Critical Assets, and its list of null CCAs. TRE_URE2 had an issue with CIP-002-2 R4 from the date the undesignated person signed the documents to the date the newly designated person signed and approved TRE_URE2's RBAM, its list of Critical Assets, and its list of null CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because from the time the plant manager signed the documents until the time the senior manager signed them TRE_URE2's methodology did not change. Moreover, TRE_URE2 did not previously have any CCAs and does not currently have any CCAs. Texas RE determined that the instant issue is appropriate for FFT treatment because it occurred around the time one TRE_URE2 affiliated company had an issue with CIP-002-1 R4, and thus is not considered a repeat violation. Also, the circumstances of the two instances of noncompliance are different.	To mitigate this issue, TRE_URE2: 1) correctly designated a senior manager; and 2) had the correctly designated senior manager sign the RBAM, its list of Critical Assets, and its list of null CCAs. To prevent re-occurrence, TRE_URE2 assigned compliance responsibility to in-house personnel rather than an outside consultant. TRE_URE2 hired a director of reliability process and compliance to improve its compliance program. TRE_URE2 updated and refined its compliance procedures for the applicable NERC standards and approving the RBAM. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3) Barney M Davis LP (BMDLP)	NCRXXXX	TRE2013012083	CIP-002-2	R4	TRE_URE3 submitted a Self-Report to Texas RE stating that it had an issue with CIP-002-2 R4. Specifically, TRE_URE3 did not have a senior manager or delegate sign its risk-based assessment methodology (RBAM), its list of Critical Assets, and its list of null CCAs. TRE_URE3 designated one person as the senior manager. TRE_URE3's plant manager, instead of the designated person, signed TRE_URE3's RBAM, its list of Critical Assets, and its list of null CCAs. TRE_URE3's plant manager had not been designated as a senior manager or delegate. TRE_URE3 designated a third person as the senior manager. TRE_URE3 had an issue with CIP-002-2 R4 from the date the undesignated person signed the documents to when the newly designated person signed and approved TRE_URE3's RBAM, its list of Critical Assets, and its list of null CCAs.	This issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because from the time the plant manager signed the RBAM, until the time the official delegate signed it, TRE_URE3's methodology did not change. Moreover, TRE_URE3 did not have any CCAs and does not currently have any CCAs. Texas RE determined that the instant issue is appropriate for FFT treatment because it occurred around the time one TRE_URE2 affiliated company had an issue with CIP-002-1 R4, and thus is not considered a repeat violation. Also, the circumstances of the two instances of noncompliance are different.	To mitigate this issue, TRE_URE3: 1) correctly designated a senior manager; and 2) had the correctly designated senior manager sign the RBAM, its list of Critical Assets, and its list of null CCAs. To prevent re-occurrence TRE_URE3 assigned compliance responsibility to in-house personnel rather than an outside consultant, TRE_URE3 a director of reliability process and compliance to improve its compliance program. TRE_URE3 updated and refined its compliance procedures for the applicable NERC standards and approving the RBAM. Texas RE has verified the completion of all mitigation activity.

Attachment A-2

June 27, 2013 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4)	NCRXXXX	TRE201100555	CIP-004-3	R4; R4.1	Following a Compliance Audit, Texas RE determined that TRE_URE4 completed quarterly reviews and maintained documentation of personnel with access to Critical Cyber Assets (CCA) and of the associated access rights for each person. However, TRE_URE4 failed to update the CCA list within seven days of any change of personnel with such access to CCA. Specifically, Texas RE determined after a review of the unescorted physical access rights list, the access control procedures, and an internal disable access order, that TRE_URE4 failed to update its CCA physical access list within seven calendar days of a contractor's CCA access rights being terminated, as required by R4.1. TRE_URE4 had an issue with CIP-004-3 R4.1 for one day, the date the change in the contractor's physical access rights were recorded, which was eight days after his access rights were terminated.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. The risk was mitigated by the short violation duration period and TRE_URE4 evidencing that the contractor's badge was surrendered to management on his last day of employment. PSP access now requires dual authentication; badging and pin number authentication.	To mitigate this issue TRE_URE4 removed the former contractor from its CCA access list. PSP access now requires dual authentication: badging and pin number authentication. Texas RE has verified the completion of all mitigation activity.
Texas Reliability Entity (Texas RE)	Unidentified Registered Entity 5 (TRE_URE5)	NCRXXXX	TRE2012011442	CIP-007-3a	R7; R7.2	TRE_URE5 submitted a Self-Report to Texas RE stating that it had an issue with CIP-007-3a R7.2. Specifically, on TRE_URE5 redeployed a server analyst workstation without erasing the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. Rather than wiping the drive device with the prescribed tool of choice, the device was re-imaged with a standard analyst workstation image. TRE_URE5 duly erased the data storage media. The issue duration is from the date the server was placed into service, through the date the server drive was properly erased.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: a) the Cyber Asset remained within the Physical Security Perimeter (PSP) at all times; and b) though TRE_URE5 re-imaged the system instead of securely erasing the system as required, sophisticated and difficult forensic tool and techniques would be required to retrieve any potential data left on the machine. Texas RE determined that the instant issue is appropriate for FFT treatment because none of TRE_URE5's prior CIP-007 violations involved disposal or redeployment of Cyber Assets.	To mitigate this issue, TRE_URE5: 1) purchased software to erase the data storage media; 2) erased the data storage media; and 3) documented the change control. Texas RE has verified the completion of all mitigation activity.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1) Grand Coulee Project Hydroelectric Authority (GCPH)	NCRXXXXX	WECC2013012408	CIP-002-3	R4	WECC performed a Compliance Audit of WECC_URE1's compliance with, among other Reliability Standards, CIP-002-3 R4. According to the WECC audit team, WECC_URE1 could not show evidence of compliance with this Standard for one calendar year. During the audit, WECC_URE1 provided copies of null lists of Critical Cyber Assets (CCAs) and Critical Assets, signed and dated by a senior manager. But WECC_URE1's risk-based assessment methodology (RBAM) had not been signed or dated. WECC_URE1 did provide evidence of compliance with the Standard for the next calendar year and provided a signed RBAM.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE1 had correctly developed null lists of its Critical Assets and CCAs and its senior manager had signed and dated the lists. Based on these actions, WECC_URE1 did not expose any Critical Assets or CCAs to a potential threat. As a compensating measure, WECC_URE1 incorporated an approval signature block for the CIP senior manager as part of its RBAM review and approval process, and for use in future RBAM criteria documentation.	To mitigate this issue, WECC_URE1: 1) provided copies of its RBAM and null lists of Critical Assets and CCAs signed and dated by a senior manager; and 2) incorporated an approval signature block for the CIP senior manager as part of its RBAM review and approval process, and for use in future RBAM criteria documentation.

Document Accession #: 20130627-5131 **Filed Date: 06/27/2013**

Document Content(s)