Federal Energy Regulatory Commission
Washington, D.C. 20426
January 13, 2022

FOIA No. FY19-30 (RC13-2)
Forty Seventh Determination
Letter (Release)

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated December 14, 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. RC13-2, along with the names of five (5) 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 RC13-2.

With respect to the remaining identities of UREs contained in RC13-2, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the

[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 appropriate.

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of UREs associated with RC13-2 will not be disclosed.

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

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

Sincerely,

BENJAMIN WILLIAMS
Digitally signed by BENJAMIN WILLIAMS
Date: 2022.01.12 10:04:29 -05'00'

Benjamin Williams
Deputy 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

November 30, 2012

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

Re: NERC FFT Informational Filing
FERC Docket No. RC13-__-000

Dear Ms. Bose:

RC13-2

New Hope Power Company (NHPP)-.pdf page 24

City of Batavia Municipal Electric Utility (City of Batavia)-.pdf page 24

Farmers' Electric Cooperative, Inc. of New Mexico (FECNM)-.pdf page 25

Sweetwater Wind 5, LLC (Sweetwater 5)-.pdf page 25

Duke Energy Generation Services, Inc. (DEGS)-.pdf page 26

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find, Fix, Track and Report[1] (FFT Spreadsheet) in Attachment A regarding 25 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 40 possible violations[5] of 16 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 40 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is an appropriate disposition of these matters, and will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards.

Statement of Findings Underlying the FFT

The descriptions of the remediated issues and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval by NERC Enforcement staff, under delegated authority from the NERC Board of Trustees Compliance Committee (NERC BOTCC), of the findings reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), each Reliability Standard at issue in this FFT is identified in Attachment A.

Text of the Reliability Standards at issue in the FFT may be found on NERC's website at http://www.nerc.com/page.php?cid=2|20. For each respective remediated issue, the Reliability Standard Requirement at issue is listed in Attachment A.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the possible violations identified in Attachment A have been mitigated. The respective Registered Entity has submitted a certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, a spot check, a random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

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

Statement Describing the Resolution[8]

Basis for Determination

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

Notice of Completion of Enforcement Action

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

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

Request for Confidential Treatment of Certain Attachments

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

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

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

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

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

Attachments to be included as Part of this FFT Informational Filing

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

a) FFT Spreadsheet, included as Attachment A; and

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

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

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

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

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

cc: Entities listed in Attachment B

NERC

Attachment a

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

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR NOVEMBER 2012
FIND, FIX, TRACK AND REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

Stacy Dochoda*
President and Chief Executive officer
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
sdochoda@frcc.com

Linda Campbell*
VP and Executive Director Standards & Compliance
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
lcampbell@frcc.com

Barry Pagel*
Director of Compliance
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 690
Tampa, Florida 33607-8402
(813) 207-7968
(813) 289-5648 – facsimile
bpagel@frcc.com

FOR MRO:

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

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

FOR NPCC:

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

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

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

FOR RFC:

Robert K. Wargo*
Director of Analytics & Enforcement
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
bob.wargo@rfirst.org

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

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

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

FOR SERC:

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

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

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

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

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

FOR SPP RE:

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

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

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

FOR TEXAS RE:

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

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

FOR WECC:

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

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

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

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

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
November 30, 2012

Take notice that on November 30, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding twenty-five (25) Registered Entities in eight (8) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Seminole Electric Cooperative (SEC)	NCR00068	FRCC2012011147	MOD-008-1	R1; R1.2	During a Compliance Audit on September 27, 2012, FRCC discovered that SEC, as a Transmission Operator, had an issue with MOD-008-1 R1. SEC's Transmission Reliability Margin Implementation Document (TRMID) did not include the description of the method used to allocate Transmission Reliability Margin (TRM) across SEC's Available Transfer Capability (ATC) Paths for the reserve sharing requirement portion of the TRM. SEC's response to an FRCC Audit data request includes a description of the method used, but that description is not included in the TRMID, as required by the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. FRCC determined that SEC was performing according to the methodology stated in the data request and all of the requirements were being met and implemented for the compliance period, but the TRMID documentation was lacking a description of the methodology.	To mitigate this issue, SEC revised its TRMID, contained within department practice *SOP-Guide-013,* to include a description of the method used to allocate TRM across SEC's ATC Paths for the reserve sharing requirement portion of the TRM. Also, SEC posted the revised TRMID to its Open Access Same-Time Information System (OASIS) website as well as to the FRCC website for operating entities, and affected entities were notified of the revised document. FRCC has verified the Mitigation Plan completion.
Midwest Reliability Organization (MRO)	Tatanka Wind Power, LLC (TWP)	NCR10245	MRO2012011005	IRO-001-1.1	R8	On September 4, 2012, TWP as a Generator Operator, self-reported an issue with IRO-001-1.1 R8 because it failed to comply with reliability directives issued by its Reliability Coordinator (RC). On July 12, 2011, Dickey County, North Dakota (where TWP is partially located) experienced severe weather and as a result transmission facilities were constrained. Therefore, TWP was under a production curtailment of varying levels per direction of its RC from July 12, 2011 until December 19, 2011 (Constrained Period). TWP's RC provided several levels of production curtailment, limiting TWP generation from 105 MW to 120 MW at different times during the Constrained Period. There were ten instances where TWP unintentionally and momentarily exceeded the production curtailment level. On average, the duration of each excursion was 6.5 minutes for 7.6 MW. The highest point of excursion was 19 MW.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TWP exceeded its production curtailment level a small number of times, ten times, for an average of 7.6 MW for 6.5 minutes. TWP is interconnected to a 230 kV transmission line and such small and short excusions (7.6 MW for 6.5 minutes) would not pose anything more than a minimal risk to the 230 kV transmission line and to the BPS. Additionally, TWP is a non-dispatchable intermittent wind generation resource, consisting of 120 1.5 MW wind turbine generators (WTGs) for an aggregate capability of 180 MW, straddling the border of North Dakota and South Dakota.	TWP has taken the following actions to minimize the reoccurrence of similar events: 1) On August 2, 2011, TWP installed two autopilot programs in order to decrease the reaction time for responding to wind speed variations, thus, assisting in keeping TWP under the production curtailment level; 2) On August 12, 2011, TWP revised the settings in the autopilot program to further improve their response time; 3) TWP implemented a protocol that requires the autopilot program to be shut down and restarted on a monthly basis to ensure that it is operating as designed, and to safeguard its effectiveness to adhering to the TWP production curtailment level; 4) TWP implemented a protocol under which its server resets are scheduled through one individual with the responsibility to ensure that TWP will not exceed production curtailment during the resets, by, among other things, ensuring that the electric system operator (ESO) has manually stopped enough WTGs at their maximum generation rating to ensure that at no time would TWP be capable of exceeding the production curtailment during the server reset; and 5) TWP purchased a new, integrated generation control system which will be more robust than autopilot because it is a product provided by TWP's software vendor and it runs on the program logic controllers and is a hardware solution. The ESO uses the supervisory control and data acquisition system only as an interface into this system, therefore resetting or rebooting the servers has no effect on generation control.
Midwest Reliability Organization (MRO)	Tatanka Wind Power, LLC (TWP)	NCR10245	MRO2012011006	TOP-001-1	R3	On October 28, 2011, TWP as a Generator Operator, self-certified an issue with TOP-001-1 R3 because it failed to comply with reliability directives issued by its Reliability Coordinator (RC). On July 12, 2011, Dickey County, North Dakota (where TWP is partially located) experienced severe weather and as a result transmission facilities were constrained. Therefore, TWP was under a production curtailment of varying levels per direction of its RC from July 12, 2011 until December 19, 2011 (Constrained Period). TWP's RC provided several levels of production curtailment, limiting TWP generation from 105 MW to 120 MW at different times during the Constrained Period. There were ten instances where TWP unintentionally and momentarily exceeded the production curtailment level. On average, the duration of each excursion was 6.5 minutes for 7.6 MW. The highest point of excursion was 19 MW.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TWP exceeded its production curtailment level a small number of times, ten times, for an average of 7.6 MW for 6.5 minutes. TWP is interconnected to a 230 kV transmission line and such small and short excusions (7.6 MW for 6.5 minutes) would not pose anything more than a minimal risk to the 230 kV transmission line and to the BPS. Additionally, TWP is a non-dispatchable intermittent wind generation resource, consisting of 120 1.5 MW wind turbine generators (WTGs) for an aggregate capability of 180 MW, straddling the border of North Dakota and South Dakota.	TWP has taken the following actions to minimize the reoccurrence of similar events: 1) On August 2, 2011, TWP installed two autopilot programs in order to decrease the reaction time for responding to wind speed variations, thus, assisting in keeping TWP under the production curtailment level; 2) On August 12, 2011, TWP revised the settings in the autopilot program to further improve their response time; 3) TWP implemented a protocol that requires the autopilot program to be shut down and restarted on a monthly basis to ensure that it is operating as designed, and to safeguard its effectiveness to adhering to the TWP production curtailment level; 4) TWP implemented a protocol under which its server resets are scheduled through one individual with the responsibility to ensure that TWP will not exceed production curtailment during the resets, by, among other things, ensuring that the electric system operator (ESO) has manually stopped enough WTGs at their maximum generation rating to ensure that at no time would TWP be capable of exceeding the production curtailment during the server reset; and 5) TWP purchased a new, integrated generation control system which will be more robust than autopilot because it is a product provided by TWP's software vendor and it runs on the program logic controllers and is a hardware solution. The ESO uses the supervisory control and data acquisition system only as an interface into this system, therefore resetting or rebooting the servers has no effect on generation control.
Reliability*First* Corporation (Reliability*First*)	American Transmission Co. LLC (ATC)	NCR00685	RFC2011001267	FAC-009-1	R1	On December 21, 2011, ATC self-reported an issue with FAC-009-1 R1 to Reliability*First,* as a Transmission Owner. On September 8, 2011, ATC commenced a project at its Butler Substation to remedy congestion issues in southeastern Wisconsin (Project). Upon completion of the Project, ATC planned to establish a rating of 1688 amps for its Granville-Butler 138 kV transmission line (Line 3453). ATC established the planned 1688 amp rating in accordance with its Facility Ratings Methodology (Methodology). The outage associated with the Project also provided ATC with an opportunity to evaluate Line 3453 pursuant to the NERC Facilities Ratings Alert. On September 9, 2011, ATC discovered a field condition on Line 3453 that required ATC to establish a more restrictive Facility Rating. The field condition ATC discovered on September 9, 2011, was a clearance to underbuild discrepancy. ATC remediated the field condition on March 28, 2012 when it lowered the underbuild at issue. Upon discovery of the field condition, ATC approved an interim rating for Line 3453 of 1420 amps consistent with its Methodology. ATC authorized the 1420 amp rating to stay in effect until May 1, 2012 to allow sufficient time to complete any necessary corrective actions in the field on Line 3453. Upon completion of the Project in late September 2011, ATC incorrectly recorded the rating for Line 3453 as 1688 amps. On October 12, 2011, ATC approved and validated the 1688 amp rating for Line 3453 and uploaded it into ATC's energy management system (EMS) and provided the rating to its Reliability Coordinator (RC). On November 3, 2011, during a closeout review of the Project, ATC identified that the 1688 amp rating was the incorrect rating for Line 3453 and that due to a discovered field condition, the rating should be 1420 amps. In response to the discovery, ATC revised its Facility Rating for Line 3453 to 1420 amps.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. First, the maximum loading of Line 3453 during the duration of the issue was 770 amps. Second, ATC has a documented Methodology which it used to determine both Facility Ratings associated with Line 3453. Finally, the issue does not indicate a systemic issue with ATC's Methodology or its application. Rather, the issue was an isolated incident which ATC immediately mitigated upon discovery.	In its Self-Report, ATC stated that on November 11, 2011, it revised its ratings on Line 3453 from 1688 amps to 1420 amps so as to be consistent with its Methodology.

Attachment A-1

November 30, 2012 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
ReliabilityFirst Corporation (ReliabilityFirst)	Northampton Generating Company (Northampton)	NCR00852	RFC2011001268	FAC-008-1	R1; R1.2	During the Compliance Audit, ReliabilityFirst discovered an issue with FAC-008-1 R1 by Northampton, as a Generator Owner. ReliabilityFirst analyzed Northampton's Facility Ratings Methodology dated August 23, 2010. ReliabilityFirst determined that this methodology did not include a specific method for rating current sensing devices, or current transformers (CTs). Instead, this methodology stated that the ratings for CTs would meet or exceed full load current. ReliabilityFirst reviewed Northampton's Facility Ratings Methodology in place prior to August 23, 2010 and determined that it contained a substantially similar statement with respect to CTs. In August of 2010, Northampton switched operating companies to NAES Corporation. As a result of this switch, Northampton modified its NERC-related programs, including its Facility Ratings Methodology.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Northampton provided commissioning test data for CTs which demonstrated that ratings for those CTs existed. The ratings were consistent with the Facility Ratings Methodology. Furthermore, throughout the pendency of this issue, Northampton maintained and implemented a Facility Ratings Methodology that considered all required elements, although the document lacked specificity regarding Northampton's consideration of CTs. Finally, Northampton designed its generator so that CTs would not limit the rating of the associated element or facility.	Northampton revised its Facility Ratings Methodology to include statements regarding the method by which it determines ratings for CTs.
ReliabilityFirst Corporation (ReliabilityFirst)	Northampton Generating Company (Northampton)	NCR00852	RFC2011001269	PRC-005-1	R1	During the Compliance Audit, ReliabilityFirst discovered an issue with PRC-005-1 R1 by Northampton, as a Generator Owner. Northampton's Protection System maintenance and testing program, submitted to demonstrate compliance with PRC-005-1 R1, stated that Northampton did not perform periodic maintenance and testing for current transformers (CTs) and potential transformers (PTs) at defined intervals. Rather, Northampton waited until a device exhibited problems and performed maintenance and testing at that time.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Northampton provided evidence demonstrating that it tested its CTs and PTs upon commissioning the generating station in 1995. Northampton had not required periodic maintenance for CTs and PTs based on recommendations from the devices' manufacturers. The manufacturer designed these particular CTs to require very little maintenance. Additionally, Northampton had summarized the maintenance and testing procedures to be applied if a CT or PT experienced a problem.	Northampton revised its Protection System maintenance and testing program to require periodic testing of CTs and PTs. Northampton also committed to complete testing on its CTs and PTs during an outage.
ReliabilityFirst Corporation (ReliabilityFirst)	Northampton Generating Company (Northampton)	NCR00852	RFC2011001270	PRC-005-1	R2	During the Compliance Audit, ReliabilityFirst discovered an issue with PRC-005-1 R2 by Northampton, as a Generator Owner. Specifically, ReliabilityFirst discovered that Northampton was missing records demonstrating that it tested its two battery systems quarterly, as required by its maintenance and testing program. Specifically, Northampton failed to produce testing records for the fourth quarter of 2008, and the first, third and fourth quarters of 2010.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Northampton provided work orders indicating that Northampton requested testing to be performed by a contractor and that such testing was scheduled for completion during the impacted calendar quarters. ReliabilityFirst considered these work orders as strong evidence that these quarterly tests did occur.	Northampton revised its procedures for maintenance and testing of batteries to more clearly delineate tasks associated with this maintenance and testing. Northampton also completed quarterly testing in accordance with these revised procedures
ReliabilityFirst Corporation (ReliabilityFirst)	Wabash Valley Power Association, Inc. (Wabash)	NCR00940	RFC2011001251	PRC-005-1	R1	On December 8, 2011, Wabash self-reported to ReliabilityFirst an issue with PRC-005-1 R1, as a Distribution Provider that owns a transmission Protection System. Wabash determined that it did not have a maintenance and testing program for Protection System devices in two of its substations that interconnect above 100 kV. The configuration of the two substations at issue is extremely rare for Wabash. In the ReliabilityFirst region, Wabash has approximately 297 points at which it is interconnected with transmission facilities owned by other utilities. Only approximately 8% of the interconnection points are operated at 100 kV or above, and only 1% of the interconnection points are operated at 100 kV or above and contain a transmission Protection System necessitating a maintenance and testing program. Specifically, Wabash has one Protection System relay and one battery system consisting of 60 battery cells at its Wheatfield substation (Wheatfield). Wheatfield provides protection from the high side of the 138 kV/12.47 kV transformer to the low side 12.47 kV station bus. Wabash's single Protection System relay at Wheatfield ties into the protection scheme operated by an interconnected utility, Northern Indiana Public Service Company (NIPSCO), thereby requiring Wabash's compliance with PRC-005-1 R1. If the Wheatfield breaker fails to operate or misoperates, it will send a trip command to two upstream NIPSCO-owned 138 kV breakers. Wabash's Northwest substation (Northwest) has one Protection System relay and one battery system consisting of 24 battery cells. Northwest also provides protection from the high side of a 138 kV/12.47 kV transformer to the low side 12.47 kV station bus, and Northwest's one Protection System relay ties into the protection scheme operated by NIPSCO in the same manner as Wheatfield.	ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk posed to the BPS was mitigated by the following factors. The extent of Wabash's issue includes two Protection System Relays and two Protection System battery systems. During the duration of the issue, Wabash contracted with a third-party to conduct maintenance and testing of its Protection System battery systems at Wheatfield and Northwest. Wabash's contractor performed maintenance and testing on its Wheatfield and Northwest Protection System battery systems annually, with the exception of Wheatfield in 2010. Testing was halted by Wabash in 2010 due to safety concerns Wabash had with the contractor. As a result of these concerns, Wabash hired a new contractor, Energy Systems Maintenance LLC, to provide testing and services in for Wheatfield in 2011 and 2012. The maintenance and testing of Protection System batteries included a visual inspection for corrosion, testing each cell for specific gravity and temperature, as well as voltage readings of each battery cell. Additionally, the two Protection System relays at issue are microprocessor relays that were monitored by Wabash and NIPSCO during the duration of the issue. As a result, NIPSCO would have had visibility into any operations issues related to these relays. Finally, there were no operational issues or misoperations of the Protection System devices at Wheatfield or Northwest during the duration of the issue.	Wabash developed a maintenance and testing program for its Protection System devices at Wheatfield and Northwest. Wabash also committed to complete maintenance and testing on its Protection System devices located at Wheatfield and Northwest pursuant to its program.

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*) and Southwest Power Pool Regional Entity (SPP RE)	American Electric Power Service Corporation as agent for Appalachian Power Company, Columbus Southern Power Company, Indiana Michigan Power Company, Kentucky Power Company, Kingsport Power Company, Ohio Power Company, and Wheeling Power Company; American Electric Power Service Corp. As Agent For Public Svc. Co. Of Oklahoma & SW Ele Pwr Co. (AEP)	NCR00682; NCR01056	RFC2012010608; SPP2012010531	EOP-008-0	R1; R1.3; R1.6	From June 11, 2012 through June 14, 2012, Reliability*First* and SPP RE conducted a Compliance Audit of AEP, during which Reliability*First* discovered an issue with EOP-008-0 R1, as a Transmission Operator (TOP). AEP performs the TOP function in Reliability*First* from two control centers in New Albany, Ohio and Roanoke, Virginia. AEP has a contingency plan to continue reliability operations in the event its control center becomes inoperable for each of these control centers. While there is a list of the critical facilities in its New Albany, Ohio contingency plan, the Roanoke, Virginia contingency plan does not include the list of the critical facilities, as required by EOP-008-0 R1.3. Also during the Compliance Audit of AEP, SPP RE discovered an issue with EOP-008-0 R1, as a Balancing Authority (BA). AEP performs the BA function in SPP RE from two control centers. AEP performs the TOP function in SPP RE from three control centers**:** one in New Albany, Ohio, one in Tulsa, Oklahoma, and one in Shreveport, Louisiana. AEP has a contingency plan for each of these control centers to continue reliability operations in the event its control center becomes inoperable. The New Albany, Ohio contingency plan did not list the TOP or BA critical facilities, as required by EOP-008-0 R1.3. In addition, the Columbus, Ohio and Shreveport, Louisiana contingency plans did not include procedures and responsibilities for providing annual training, as required by EOP-008-0 R1.6.	Reliability*First* and SPP RE determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. Regarding EOP-008-0 R1.3, although the list of critical facilities was not in the contingency plans, the list of critical facilities did exist and was located in the New Albany, Ohio contingency plans. Although there are separate contingency plans for separate control centers, this plan included the list of all critical facilities. Regarding EOP-008-0 R1.6, although the requirement to provide training was not in the contingency plans, AEP provided evidence that it completed the required annual training.	AEP revised the New Albany, Ohio plan to include a list of critical facilities. In addition, AEP revised its Tulsa, Oklahoma and Shreveport, Louisiana plans to include procedures and responsibilities for providing annual training. AEP posted each of the plans to the Transmission Operations SharePoint site so that its transmission operators and dispatchers have access to it.
SERC Reliability Corporation (SERC)	Hot Spring Power Company, LLC (Hot Spring)	NCR01257	SERC2012010982	PRC-005-1	R2	On August 28, 2012, Hot Spring, as a Generator Owner, self-reported an issue with PRC-005-1 R2, stating that during an internal assessment of Hot Spring's Protection System, it could not locate documentation for the 2008 interval for capacity load testing of the two Valve Regulated Lead Acid (VRLA) batteries. Hot Spring located a work order from March 2008 that indicated capacity load testing had been performed, but vendor test records do not include capacity load tests. Hot Spring subsequently tested both batteries twice within the defined intervals. SERC reviewed a spreadsheet compiled by Hot Spring providing a complete inventory of its Protection System devices, with defined intervals, and maintenance and test dates for the most current and previous dates listed for each Protection System device. SERC verified the assigned intervals based on a review of Hot Spring's Protection System maintenance and testing procedure, ensuring consistency with the listed intervals provided in the spreadsheets. Based on this review, SERC determined that Hot Spring failed to have test or maintenance records for two out of three station batteries (66.6%). In total, Hot Spring failed to have test or maintenance records for two out of 229 Protection System devices (0.87%).	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) Hot Spring's battery charger and DC system has basic alarming in the control system. These alarms are part of a supervisory control and data acquisition system that allows the operators to monitor the alarms continuously 24 hours a day, seven days a week. This alerts personnel to a battery or charger failure; 2) Hot Spring conducted monthly and annual inspections and maintenance on the batteries, including voltage check, grounds detection and electrolyte levels and found no issues; and 3) Hot Spring's plant is a merchant power plant and does not have a long term contract in place.	SERC verified that Hot Spring conducted capacity load testing of all batteries in December 2010 and November 2011.
SERC Reliability Corporation (SERC)	Hot Spring Power Company, LLC (Hot Spring)	NCR01257	SERC2012010983	PRC-005-1	R1	On August 28, 2012, Hot Spring, as a Generator Owner, self-reported an issue with PRC-005-1 R1, stating that Hot Spring's Protection System maintenance and testing procedure did not include associated communication systems (ACS) devices. Although Hot Spring does not own ACS devices, its Protection System maintenance and testing procedure does not include a statement to that effect. SERC reviewed Hot Spring's Protection System maintenance and testing procedure and verified that it included protective relays, voltage and current sensing devices, batteries, and DC control circuitry, including the maintenance and testing intervals and their basis, and a summary of maintenance and testing for each of these device types. SERC also verified that Hot Spring did not address ACS devices in its Protection System maintenance and testing procedures until April 1, 2011, when it included a statement that it did not own ACS devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the only omission from Hot Spring's Protection System maintenance and testing procedure was a statement that Hot Spring does not own any ACS devices.	SERC verified that Hot Spring revised its Protection System maintenance and testing procedure to include a statement that Hot Spring does not own ACS devices.
SERC Reliability Corporation (SERC)	Sabine River Authority of TX/LA (Sabine)	NCR01305	SERC2011007292	PRC-005-1	R1	On May 25, 2011, Sabine, as a Generator Owner (GO), self-reported an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program did not include maintenance and testing intervals and their basis, or a summary of maintenance and testing procedures for all Protection System devices. Sabine self-reported this issue after being informed by the Generator Operator (GOP) that SERC had identified deficiencies in the GOP's Protection System maintenance and testing procedure, which Sabine used for its GO function along with internal Sabine procedures. Sabine's and the GOP's Protection System maintenance and testing procedures that were in effect at the beginning of the compliance period did not include the summary of maintenance and testing for the batteries or DC control circuitry devices. Sabine did not have battery maintenance and testing procedures until 2009. In addition, Sabine's maintenance and testing procedures did not address Associated Communication System (ACS) devices. Although Sabine does not have any ACS devices, neither its internal procedure nor that of the GOP noted that fact.	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) Sabine's generator Protection System devices were being maintained and tested through the GOP's automated maintenance management system, which identified, tracked, and documented completion of maintenance and testing of the Protection System devices using work orders. This system also identified the test intervals and due dates to ensure that the Protection System devices were scheduled and tested at the appropriate date. The work order issued by this system contained the necessary procedures and technical information to conduct maintenance and testing for each relevant Protection System device; and 2) Since Sabine does not have any ACS devices, the omission of this Protection System device type was not significant.	SERC verified that Sabine completed the following actions: 1) Sabine's personnel conducted an in-depth review to improve their understanding of the requirements of the Standard and scheduled an annual review of the requirements of the Standard; 2) Conducted a complete review of Sabine's GO facilities with the GOP and verified that all Protection System components have been included in the inventory as required by the Standard; 3) Developed a separate Protection System maintenance and testing procedure for its Transmission Facilities that includes the maintenance and testing intervals and their basis and a summary of maintenance and testing for all its Transmission Owner (TO) Protection System devices; 4) Revised its Protection System maintenance and testing procedure for its Generation Facilities to include maintenance and testing intervals and their basis and a summary of maintenance and testing and a statement that Sabine owns no ACS devices that require testing; 5) Added the components that had been omitted from the Protection System maintenance and testing program to the maintenance and testing program that tracks and schedules future testing of the components; 6) Conducted a complete review of the TO facilities with the Transmission Operator (TOP) and verified that all components have been included in the inventory as required by the Standards; and 7) Revised the current Protection System maintenance and testing preventative maintenance basis document to outline the basis for testing the TO components that aligns with the TOP's maintenance and testing program.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Sabine River Authority of TX/LA (Sabine)	NCR01305	SERC2011007293	PRC-005-1	R2	On May 26, 2011, Sabine, as a Generator Owner (GO), self-reported an issue with PRC-005-1 R2 stating it could not provide evidence all Protection System devices were maintained and tested within the defined intervals and the date each Protection System device was last tested or maintained. SERC reviewed spreadsheets prepared by Sabine that included each of Sabine's Protection System devices for its GO and Transmission Owner (TO) registrations and the defined maintenance and testing intervals, the most recent test date and the previous test date for each device. SERC reviewed test dates for all test periods since the beginning of the enforceable period. SERC verified the assigned intervals based on a review of Sabine's Protection System maintenance and testing procedures ensuring consistency between the listed intervals provided in the spreadsheets and those included in Sabine's procedures. SERC determined that Sabine tested one out of one station batteries (100%) outside of interval and failed to have previous testing or maintenance records for 24 out of 68 voltage and current sensing devices (35.3%). In total, SERC determined that Sabine was non-compliant for 25 out of 157 Protection System devices (15.9%).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1) Sabine's maintenance contractor provided email records stating that the battery monthly tests were performed during the three months with missing records, but these specific records were lost or misplaced. Sabine reviewed the monthly battery test records for the months before and after each missing record and found no abnormalities with the battery system; 2) Sabine was up to date with all of its Protection System device maintenance and testing activities by March 31, 2011 and Sabine found no issues with the missed Protection System devices; and 3) Sabine is an 81 MW hydro station which operates intermittently for a few hours each day Monday through Friday based on the reservoir water level. It is not dispatched at any other times, and is not considered a critical asset to the reliability of the BPS. Power generated is routed to a single 138 kV step-up transformer then through a 138 kV substation that is tied to an adjacent utility.	SERC verified that Sabine completed the following actions: 1) Sabine's personnel conducted an in-depth review to improve their understanding of the requirements of the Standard and scheduled an annual review of the requirements of the Standard; 2) Conducted a complete review of Sabine's GO facilities with the Generator Operator and verified that all Protection System components have been included in the inventory as required by the Standard; 3) Added the components that had been omitted from the Protection System maintenance and testing program to the maintenance and testing program that tracks and schedules future testing of the components; 4) Performed the required tests on the components determined to be out of compliance and obtained copies of the reports verifying the work was performed and components are functioning properly; 5) Conducted a complete review of the TO facilities with the Transmission Operator and verified that all components have been included in the inventory as required by the Standards; and 6) Reviewed maintenance contractor documentation of component testing and verified they provide sufficient detail to meet the Standard.
SERC Reliability Corporation (SERC)	Tenaska Alabama Partners, L.P. (Tenaska-AL)	NCR01335	SERC2011007288	VAR-002-1.1b	R3	On May 24, 2011, Tenaska-AL, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3, stating that on May 10, 2011, the control room operator observed that the power system stabilizers (PSS) on three units were in the "Off" position. The operator then changed the PSSs to the "On or Armed/Active" position and notified Plant Management. However, Tenaska-AL did not notify the appropriate Transmission Operator (TOP) within 30 minutes of the change in PSS status as required by VAR-002-1.1b R3. Further investigation by Tenaska-AL determined that two units had their respective PSSs in the "Off" position. SERC requested and reviewed additional documents in order to complete its assessment. Tenaska-AL operates Lindsay Hill Generating Station, which has three combustion turbines (CT1, CT2, and CT3), and one steam turbine, with a total rating of 1,041 MVA for the station (199 MVA for each CT and 444 MVA for the steam turbine). SERC learned that Lindsay Hill Generating Station is located adjacent to a generating station with an approximate capacity of 885 MW. The two plants monitor and coordinate the MVAR/MW ratio with each other to control the switchyard voltage that is common to both plants. SERC determined that Tenaska-AL operated the CT1 and CT3 units with their respective PSSs off. On May 4, 2011, Tenaska-AL started and released the CT1 unit to the grid system with its PSS off. On May 10, 2011, after realizing that the PSS was in the incorrect position, the operator turned it on but did not notify the TOP within 30 minutes of the change in PSS status. Tenaska-AL operated the CT1 unit several times with the PSS off between May 4 and May 10, 2011 for a total of approximately 33 hours. On May 9, 2011, Tenaska-AL started and released the CT3 unit to the grid system with its PSS off. On May 10, 2011, after realizing that the PSS was in the incorrect position, the operator turned it on but did not notify the TOP within 30 minutes of the change in PSS status. Tenaska-AL operated the CT3 unit several times with the PSS off between May 9 and May 10, 2011 for a total of approximately 18 hours. During this time, Tenaska-AL started and released the steam turbine and CT2 unit to the grid, on May 4 and May 10, 2011, respectively, with their PSSs turned on.	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) While the CT1 and CT3 units were online with their respective PSSs off, the steam turbine was operating with its PSS on and was controlling the voltage; 2) The Tenaska-AL facility control room is manned by a control room operator who is responsible for maintaining the plant voltage schedule provided by the TOP. The facility is located adjacent to another generating station with an approximate capacity of 885 MW. The two plants monitor and coordinate the MVAR/MW ratio with each other to control the voltage at a switchyard common to both plants; and 3) During the seven days it operated the units with their PSSs off, Tenaska-AL operated the CT1 unit for approximately 33 hours and CT3 for approximately 18 hours.	SERC verified that Tenaska-AL completed the following actions: 1) Provided instructions to all of the control room operators to verify the status of the PSSs during shift turnover and prior to starting any generator; 2) Installed alarms on the plant control system to alert the operator when any PSS control is in the "Off" position; 3) Provided written instructions to all plant personnel specifically highlighting that, when the status of the PSS changes, the TOP must be provided notification of both the status change and expected duration within 30 minutes; 4) Completed program changes that added a start permissive to each turbine requiring the PSS to be in the "Armed\Active" position in order to start the unit; 5) Created a poster and placed it in the control room to provide a quick reference to the operators by detailing when communication with the TOP is required. This poster was reviewed individually with all of the operators during their normal shifts; 6) Added requirements to the board reviews for all plant operators that plant operators explain what events require them to communicate with the TOP as well as what the communication must include, including the need to communicate the change in state and expected duration to the TOP within 30 minutes, name the items listed on the control room poster, and explain what must be done if the TOP communications are not done properly; 7) The plant manager and plant engineer reviewed the event with other plants during regularly scheduled calls with plant managers and the NERC Compliance Committee; 8) The plant manager reviewed the incident with all plant employees at scheduled monthly safety meetings; and 9) Submitted an event report to Operations management in Omaha to be forwarded to all Tenaska plants to prevent this type of event from occurring at the other plants.
Southwest Power Pool Regional Entity (SPP RE)	Midwest Energy, Inc. (Midwest)	NCR01118	SPP2012010123	EOP-008-0	R1 (R1.5, R1.6)	During a Compliance Audit of Midwest, conducted from April 24, 2012 to April 26, 2012, SPP RE identified non-compliance with EOP-008-0 R1.5 and R1.6. The Midwest's plan for loss of control center functionality (Plan) required the deployment of field personnel to critical facilities for the purpose of communicating field conditions back to operations staff. The Plan also provided in part, "[o]n an annual basis[,] System Operators and other assigned personnel will be subjected to a review of the process and procedures to be implemented in the event the Primary Control Center is lost." SPP RE determined that an annual training session and table top exercise were conducted with operations staff in accordance with the Plan. However, field personnel did not participate in the training session, did not participate in the communication exercises with operations staff, and were not deployed to the critical facilities. This remediated issue applies to Midwest's Transmission Operator function.	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 operations staff charged with overseeing the Plan implementation were trained in the Plan implementation, underwent a table top exercise, and were prepared to respond in an emergency situation. Therefore, the individuals charged with managing the Plan implementation were prepared to respond in an emergency situation. Additionally, the referenced field personnel at issue are the same individuals that inspect the critical facilities on a monthly basis. Therefore, the field personnel are familiar with the location of the critical facilities and where to gather any data requested by the operations staff. The role of the field personnel in the Plan implementation is limited to critical facility site deployment and the recording and reporting of system data to operations staff.	Midwest amended its Plan to require that "System Operators not working the desk will test the plan . . . by deploying Substation Technicians [(field personnel)] to the appropriate locations. Testing of all data and voice links at the service center will be conducted by the System Operator[s] as a part of the test." Midwest also conducted training on the new procedure and carried out a drill involving both operations and field personnel. This drill included deployment of the field staff to critical facilities and involved two-way communication between the operations staff at the back-up facility and field personnel at the critical substations.
Southwest Power Pool Regional Entity (SPP RE)	The Empire District Electric Company (EDE)	NCR01155	SPP201000339	TOP-002-2a	R11	On July 27, 2010, EDE submitted a Self-Report for noncompliance with TOP-002-2a R11 because it was no longer performing current and next-day Bulk Electric System studies consistent with the requirements of TOP-002-2a R11. EDE had previously relied on the Southwest Power Pool Reliability Coordinator (SPP RC) to perform its current and next-day studies. The SPP RC had informed EDE that although it would continue to perform system current and next-day studies, these studies would not be performed on EDE's behalf. Because there was no agreement between SPP RC and EDE to perform the studies, the SPP RC was not obligated to do so and EDE could not rely on the SPP RC to perform EDE's current and next-day studies. This remediated issue applies to EDE's Transmission Operator function.	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 the SPP RC stated that it was not performing current and next-day studies on EDE's behalf, the SPP RC continued to perform system current and next-day studies and these studies were available to EDE. EDE had trained its system operators to review the contingency analysis studies that were provided by the SPP RC and continued to establish System Operating Limits (SOLs) utilizing the SPP RC studies. EDE provided SPP RE with evidence that it not only reviewed the SPP RC studies on a daily basis, but also communicated with the SPP RC regarding the identification of SOLs.	EDE entered into a formal agreement with SPP RC whereby the SPP RC would perform next day, current day, and seasonal studies for EDE. Additionally, EDE modified its policies and procedures to incorporate the formal agreement, and to educate system operators on their responsibilities as a result of the formal agreement, including the daily documented review of the studies.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc (Texas RE)	Pattern Gulf Wind LLC (Pattern Gulf)	NCR11020	TRE201100551	PRC-005-1	R2	On November 2, 2011, Pattern Gulf Wind, as a Generator Owner (GO), self-certified an issue with PRC-005-1 R2 and subsequently self-reported the same issue on November 8, 2011. Pattern Gulf purchased the generation facility at issue, from Texas Gulf Wind and ownership was transferred on March 17, 2010. The previous owner, Texas Gulf Wind, did not provide any documentation to support the implementation of a Protection System maintenance and testing program (Program) prior to the asset being owned by Pattern Gulf. There were no maintenance and testing records available from July, 13, 2009 to March 17, 2010. Upon the ownership change, the implementation of the Program could be documented, as required. However, the actual execution of all maintenance and testing was contracted to BluArc Management Group until December 17, 2010. Therefore, from March 17, 2010 to December 17, 2010, weekly maintenance and tests were not documented. The remediated issue period was from March 16, 2010, the date Pattern Gulf was registered as a GO, to December 17, 2010, the date Pattern Gulf can show supporting documentation of operational maintenance in place.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because BluArc Management Group had provided an attestation that testing was being done during the remediated issue period despite the lack of documentation. Pattern Gulf had shown that it was performing comprehensive system maintenance and testing from December 17, 2010 onwards.	On December 17, 2010, a new Facility Manager and Assistant Facility Manager were put in charge of the facility. The Assistant Facility Manager is in charge of execution of all maintenance and testing and proper documentation of all executed maintenance and testing reports. The Facility Manager oversees and verifies proper execution and documentation of all maintenance and testing. With the new management on site, all of the maintenance and testing is executed within the intervals in accordance with the Program and properly documented. All mitigating activities have been verified as complete by Texas RE.
Texas Reliability Entity, Inc (Texas RE)	Pattern Gulf Wind LLC (Pattern Gulf)	NCR11020	TRE2012010269	PRC-018-1	R3	On May 14, 2012, Pattern Gulf, as a Generator Owner (GO), self-reported an issue with PRC-018-1 R3. During a pre-audit assessment, Pattern Gulf discovered that the owner of the Disturbance Monitoring Equipment (DME) installed in the Pattern Gulf substation was using a different piece of equipment for disturbance monitoring than Pattern Gulf had been reporting to the Regional Reliability Organization, in this case the Electric Reliability Council of Texas (ERCOT). As a result, Pattern Gulf did not maintain and report the correct piece of equipment to ERCOT, as per the regional requirement and as required by PRC-018-1 R3. The remediated issue violation period was from March 16, 2010, the date Pattern Gulf was registered as a GO, to May 10, 2012, the date the error was discovered and corrected.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because it was an administrative issue concerning the proper identification of assets assigned to record system disturbances. Pattern Gulf began reporting the correct DME information to ERCOT as of May 10, 2012. The incorrect device was being reported to ERCOT for system disturbance monitoring, even though the correct equipment was in place and fully functional. However, if information was required to report a disturbance, the Pattern Gulf technicians knew to use the correct relay installed to provide this function. Documents from Pattern Gulf show that the DME (SEL-311L) used for event and fault recording was in service during the time of the alleged violation. Once Pattern Gulf realized its mistake, it began reporting to ERCOT the correct information on the SEL-311L that was actually performing the task of disturbance monitoring and recording.	Pattern Gulf has reviewed the relay specifications and verification of the relays capabilities. The DME devices (relays) at the facility meet the requirements and are available to monitor the facility and disturbances and to record disturbance data that can and will be provided to the RC as requested, and are tested and maintained properly.
Texas Reliability Entity, Inc (Texas RE)	Tenaska Gateway Partners LTD (Tenaska)	NCR04137	TRE201100483; SPP2011008312	PRC-005-1	R2	On October 12, 2011, Tenaska, as a Generator Owner (GO), self-reported to Texas RE and SPP RE that Tenaska did not have documentation to verify the maintenance and testing of all DC control circuitry. Although maintenance and testing occured at defined intervals on most of the Protection System components at Tanaska's plant, testing of the DC control circuitry hads not been performed and documented in a manner sufficient to demonstrate compliance with PRC-005-1 R2. Tenaska follows the National Electrical Testing Association's (NETA) maintenance testing specifications for testing of its Protection System components. This remediated issue applies to 36 DC circuits, out of a total 384 Protection System devices (9.37%). The remediated issue period was from June 28, 2007, the date of Tenaska's registration as a GO, to May 1, 2012, the day that DC Circuit tests were 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) because Tenaska had been performing tests and maintenance on its remaining Protection System equipment (i.e. relays, batteries, communication systems, and Current Transformers and Potential Transformers. Also, Tenaska used relay events and successful equipment starts as evidence of functional testing of the DC control circuitry at issue. Moreover, the remediated issue applied to 9.37 % of Tenaska's Protection System Devices, thereby reducing the risk to the BPS. Additionally, when Tenaska did perform tests on its DC control circuitry, all units were deemed to be operating properly. Furthermore, Tenaska reviewed all plant Protection System operations and did not identify any misoperations during the pendency of this remediated issue.	Tenaska had identified and written procedures for all untested DC circuits, sent out and received bids for contracting the testing, and lastly, performed the required tests. All mitigating activities have been verified as complete by Texas RE.

Attachment A-2

November 30, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1) New Hope Power Company (NHPP)	NCRXXXXX	FRCC2012010994	CIP-002-1	R1; R1.2.1	During a CIP Audit, FRCC determined that FRCC_URE1 had an issue with CIP-002-1 R1. Specifically, the evidence submitted by FRCC_URE1 was insufficient to demonstrate that FRCC_URE1 considered control centers and back-up control centers in its risk-based assessment methodology (RBAM) for a period of approximately two and a half years. Although FRCC_URE1 does not own any control centers or back-up control centers, FRCC_URE1 failed to consider them in its RBAM, as required by CIP-002-1 R1.2.1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). FRCC_URE1 considered all asset types required by CIP-002 R1, based on an inventory of all BPS assets it owned and did not consider control centers as it does not own control centers or a back-up control center.	To mitigate this issue, FRCC_URE1 updated its RBAM and the procedure to include control centers and back-up control centers.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012009952	CIP-005-3a	R1; R1.5	MRO_URE1 self-reported an issue with CIP-005-3a R1.5 because it failed to afford Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter the protective measures specified in CIP-007-3 R3 (security patch management). MRO_URE1 failed to properly assess five patches within 30 days, for devices used in the control and monitoring of electronic access points. Upon assessment, MRO_URE1 reported that none of the patches were applicable to its devices. Two of the patches were assessed on the 31st day (one day beyond the required 30 days). One patch was assessed on the 63rd day (33 days late). Another patch was assessed on the 86th day (56 days late). Finally, the fifth patch was originally incorrectly assessed as applicable and then correctly assessed as not applicable 73 days later. The patches were not assessed for over three months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. MRO_URE1 has a documented patch management process which includes several layers of review. MRO_URE1 assessed 49 patches during the issue time period. After completing this process, MRO_URE1 had only failed to assess a small percentage of its total number of patches (10%). Additionally, none of the patches were applicable to MRO_URE1's devices and the duration of issues was an average of 32 days. Furthermore, MRO_URE1 discovered, mitigated and self-reported this issue due to internal audit controls.	Meetings between MRO_URE1's IT and MRO_URE1's NERC CIP leadership are now held every two weeks to discuss outstanding patch applicability assessments. This meeting will achieve leadership engagement and will prevent reoccurrence of delayed applicability assessments. Additionally, MRO_URE1 has added two escalation notifications, as well as recipients to the existing notifications. At 15 calendar days past the release, the subject matter expert and the team lead for the affected infrastructure group are added to the notification. At 21 and 28 days, additional layers of leadership are added to the notification. This is an ongoing control that will remain implemented.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012009853	CIP-004-3	R4; R4.2	NPCC_URE1 self-reported an issue with CIP-004-3 R4.2. NPCC_URE1 failed to timely revoke unescorted physical access to Physical Security Perimeters (PSPs) containing Critical Cyber Assets (CCAs). Specifically, an employee transferred to a job that no longer required unescorted access, but the employee's access rights were not revoked until 11 days after the transfer. The Standard requires the employee's access to be revoked within seven calendar days. The action to revoke because the employee no longer required access was not communicated in a timely manner to staff responsible for revoking access.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The employee transferred from working within the PSP to being a field worker. During the 11-day period, the access logs show that the employee did not access the PSPs. The transferred employee was reassigned to another part of the company where he assumed the responsibility of his newly-appointed position. During the 11-day period, the transferred employee was receiving training associated with his new position. The employee had undergone a personnel risk assessment and had previously received training concerning the responsibilities of unescorted physical access to PSPs containing CCAs.	To mitigate this issue, NPCC_URE1 completed the revocation 11 days after the employee transferred. NPCC_URE1 will prevent or minimize the risk of inconsistencies in the implementation of NPCC_URE1's access control procedures by providing additional training for all staff responsible for the implementation of NPCC_URE1's access control procedures and issuing a guidance document to responsible staff regarding initiating and revoking user access rights.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2012010642	CIP-006-3c	R1; R1.6.2	NPCC_URE1 self-reported an issue with CIP-006-3c R1.6.2. NPCC_URE1 reported that an unescorted employee-in-training was in the Physical Security Perimeter (PSP) without having authorized unescorted access to Critical Cyber Assets. The PSP access door's locking mechanism was not functioning properly. The unauthorized employee was in the PSP removing garbage for a period of seven minutes before exiting 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. NPCC_URE1's security command post received an alarm for "invalid access group" indicating a denial of access from the card key reader at the control room door for an access attempt by an unauthorized employee. This alarm was immediately followed by a "forced door" alarm. Security's response and investigation into these alarms determined that the previously-tested PSP access door's locking mechanism was no longer functioning properly, which allowed the PSP access door to be pushed open. During the period that the PSP access door's physical locking mechanism was not functioning properly, the involved PSP area was continuously occupied by a number of staff members with authorized access. Lastly, the unauthorized employee that entered the PSP had satisfied the conditions precedent to being authorized for access to the PSP, although he was not actually authorized. The employee had both a valid personnel risk assessment and had taken the mandatory CIP cybersecurity 2012 training course.	To mitigate this issue, NPCC_URE1 stationed a security officer at the PSP door until it was repaired. NPCC_URE1 also conducted training covering specific information on this incident and actions to adhere to in the future should similar situations occur. NPCC_URE1 conducted a staff meeting to improve awareness of NERC CIP and physical security. NPCC_URE1 conducted an inspection of PSP access points for signage identifying the area as restricted/limited access requiring authorization or an escort, and if needed, posted additional signage.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012011151	CIP-007-3	R6; R6.4	NPCC_URE2 self-reported an issue with CIP-007-3 R6.4. NPCC_URE2 incurred a problem with two Cyber Assets not forwarding their logs from the backup control center to the server at the new control center for a period of 90 days. A firewall located between the new control center and the former control center blocked the communication to the server at the former control center.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system due to the redundancy of the LANs at the control centers. Also, during this period the daily operations were handled by the a control center. The backup control center is a dedicated site with assets that are ready to handle operations if the operations at the other control center are compromised. If backup control center operations were required, a type of LAN was in operation with no loss of visibility. These two assets were functioning and were logging (to themselves), but were not forwarding their logs to the server, which resulted in a log retention problem. The absence of a router or switch log will not prevent a system operator from performing his duties.	To mitigate this issue, NPCC_URE2 moved the server. This move eliminated the firewall block between both the new and former control centers. NPCC_URE2 also updated its control test plan documentation to include a section requiring verification that logging is working successfully as a result of any changes to Critical Cyber Assets.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1) City of Batavia Municipal Electric Utility (City of Batavia)	NCRXXXXX	RFC2012010409	CIP-003-3	R2	RFC_URE1 self-certified an issue with CIP-003-3 R2. The CIP senior manager has been performing the role and functions as required in CIP-003-3 R2, but RFC_URE1 failed to properly identify the senior manager by name, title and date of designation in a cyber security policy procedure, as required by CIP-003-3 R2.1.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The CIP senior manager was performing the role and functions as required by CIP-003-3 R2 even though this designation was not documented in a cyber security policy procedure, as required by the Standard. In addition, RFC_URE1 has no Critical Assets.	RFC_URE1 created and implemented a procedure to identify the CIP senior manager by name, title and date of designation and included a delegate.

Attachment A-2
November 30, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP)

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010102	CIP-007-3	R4	RFC_URE2 self-reported an issue with CIP-007-3 R4 to Reliability*First* . RFC_URE1 has in place a process for the update of anti-virus and malware prevention signatures that includes testing and installing the signatures. RFC_URE2's system administrator, however, failed to test the signatures for four electronic access control and/or monitoring systems prior to installing the signatures. The system administrator failed to follow RFC_URE2's change management procedures, which did not authorize updates to these systems without testing the signatures.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. RFC_URE2 self-identified this issue and the systems at issue do not provide control functions for the BPS. In addition, RFC_URE2 has in place a process for the update of anti-virus and malware prevention signatures. In this case, an individual failed to follow the process in this isolated instance. Further, the systems at issue are located behind firewalls with access rules restricting the traffic allowed to pass to and from the systems.	RFC_URE2 created a management position to provide additional oversight of certain CIP-related processes, including change management. This manager will perform reviews of changes prior to implementation to help ensure compliance with the CIP Reliability Standards. In addition, during formal training for necessary personnel, RFC_URE2 reinforced the CIP Reliability Standards and the documented RFC_URE2 procedures.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010417	CIP-005-3a	R1	RFC_URE2 self-reported to Reliability*First* an issue with CIP-005-3a R1. RFC_URE2 placed a new electronic access control and monitoring system into service. The servers supporting this system exist on a virtual platform. The virtual platform allows multiple operating systems, or "guests," to operate concurrently on one host server. RFC_URE2 conducted and documented security patch evaluations for all guest operating systems residing on the virtual platform. RFC_URE2, however, failed to assess two security patches for the devices that run the virtual platform, operating on the physical server, which are Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter, within 30 calendar days of availability of the patches, as required by CIP-007-3 R3.1. RFC_URE2 therefore installed the patches without assessing them for applicability.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. RFC_URE2 self-identified this issue, and the systems at issue do not provide control functions for the BPS. RFC_URE2 affords these systems, which are located within the Physical Security Perimeter, the remaining protections specified in CIP-005-3a R1.5.	To address the issue that involved CIP-007-3 R4, RFC_URE2 added a review of software security advisories to its existing patch identification processes for its operating systems. The process requires an assigned individual to obtain all advisories as they are issued, and then the individual reviews each advisory for the severity level within 30 days using a spreadsheet for tracking. In addition, RFC_URE2 created a management position to provide additional oversight of certain CIP-related processes, including patch management. During formal training for necessary personnel, RFC_URE2 reinforced the CIP Reliability Standards and the documented RFC_URE2 procedures. To address the issue that involved CIP-007-3 R8, RFC_URE2 updated its cyber vulnerability assessment procedure to guide the third-party or internal tester in performing the assessment. In addition, RFC_URE2 completed the cyber vulnerability assessment.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010418	CIP-004-3	R4	RFC_URE2 self-reported to Reliability*First* an issue with CIP-006-3c R2.2. Reliability*First* assigned this CIP-006-3c R2.2 issue a tracking number, RFC2012001321. The Self-Report also indicated an issue with CIP-004-3 R4. Reliability*First* , however, did not assign a new tracking number. Instead RFC_URE2 self-certified the issue with CIP-004-3 R4 to Reliability*First.* A RFC_URE2 employee who had authorized unescorted physical access to a Physical Security Perimeter (PSP) no longer required such access. RFC_URE2 failed to disable the employee's physical access to an emergency exit from the PSP within seven calendar days. This error occurred because the name of the emergency exit did not match the name of the other doors in the PSP. RFC_URE2 revoked the employee's access.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The employee at issue transferred departments within RFC_URE2. RFC_URE2 monitors the door through badge access and visual monitoring, and the door is only accessible through a vacant adjacent room that itself is only accessible through a door that is normally locked when unattended. RFC_URE2 revoked the employee's access from all other entrances to the PSP, as well as the employee's authorized cyber access. As a result, it is unlikely that the individual would have gained access unnoticed through this door and cause harm to the integrity of the Critical Cyber Assets. Furthermore, RFC_URE2 discovered this issue during one of its periodic entitlement reviews of physical security access privileges, and the employee had a valid personnel risk assessment and cybersecurity training.	RFC_URE2 revoked the employee's authorized unescorted physical access to the emergency exit door and changed the name of the emergency exit to conform with the rest of the entrances to the PSP.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012010443	CIP-007-1	R8; R8.2; R8.3	Reliability*First* conducted a Compliance Audit of RFC_URE2 during which Reliability*First* discovered an issue with CIP-007-1 R8 by RFC_URE2. A third-party vendor performs RFC_URE2's cyber vulnerability assessment of the Cyber Assets within the Electronic Security Perimeter (ESP). RFC_URE2's third-party vendor deleted the detailed evidence related to the cyber vulnerability assessment. As a result, RFC_URE2 provided a summary report from the third-party vendor that it: (a) performed a review to verify that only ports and services required for operations for Cyber Assets within the ESP were enabled (R8.2); and (b) included a review of controls for default accounts (R8.3). RFC_URE2, however, was unable to provide detailed evidence to support the summary report.	Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. A third-party vendor performs RFC_URE2's cyber vulnerability assessment of the assets used in the access control and monitoring of the ESP. RFC_URE2's third-party vendor deleted the detailed evidence related to the cyber vulnerability assessment. As a result, RFC_URE2 provided a summary report from the third-party vendor that it: (a) performed a review to verify that only ports and services required for operations for Cyber Assets within the ESP were enabled; and (b) included a review of controls for default accounts. RFC_URE2's evidence was simply inadequate to demonstrate the extent of RFC_URE2's cyber vulnerability assessment.	RFC_URE2 updated its cyber vulnerability assessment procedure to guide the third-party or internal tester to perform the assessment. In addition, RFC_URE2 completed the annual cyber vulnerability assessment
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1) Farmers' Electric Cooperative, Inc. of New Mexico (FECNM)	NCRXXXXX	SPP201100647	CIP-002-1	R1.1	During a SPP RE CIP Compliance Audit of SPP RE_URE1, the SPP RE CIP audit team identified an instance of noncompliance with CIP-002-1 R1.1. Specifically, the CIP audit team observed that SPP RE_URE1's risk-based assessment methodology (RBAM) for identifying Critical Assets did not include evaluation criteria for assessing Critical Assets.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1's RBAM did not include evaluation criteria, SPP RE_URE1 did have a documented RBAM that it used to identify its Critical Assets. The original RBAM still considered the assets listed in CIP-002-1 R1.2 and SPP RE_URE1 determined that it did not have any Critical Assets or Critical Cyber Assets using the original RBAM.	SPP RE_URE1 revised its RBAM to include evaluation criteria for Critical Asset identification.
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1) Sweetwater Wind 5, LLC (Sweetwater 5)	NCRXXXXX	TRE201100506	CIP-002-1	R1.2.1	A Compliance Audit of TRE_URE1 resulted in the finding that TRE_URE1 had a risk-based assessment methodology (RBAM) that did not consider reliability-related to its function services. The services were provided by and performed by its qualified scheduling entity (QSE). Specifically the RBAM did not consider the QSE's control center and backup control center. This remediated issue period was from the date TRE_URE1 was required to be compliant with the Standard, to when a revised RBAM was issued.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the RBAM did not consider the control center and backup control center of TRE_URE1's QSE, the Critical Asset identification process employed by TRE_URE1 for CIP-002-1 R2 did include the control center and backup control center at issue. Additionally, the QSE did not have any direct control over the physical operation of the facility. The QSE served only as a communication conduit. Communications could have been accommodated by the facility alone in the event of loss of communications by the QSE control center and the backup control center.	TRE_URE1 issued a revised RBAM that considered the QSE control center and backup control center. All mitigating activities have been verified as complete by Texas RE.

Attachment A-2

November 30, 2012 Public CIP - Find, Fix, Track and Report Informational Filing of Remediated Issues Spreadsheet

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

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE2012011192	CIP-004-1	R4	During an Audit, a review of TRE_URE2's original personnel Critical Cyber Assets (CCA) access list revealed that the list did referenced general electronic access rights, but lacked the required electronic access rights specific detail. The original list simply stated if an employee had electronic access rights but not the scope of their specific rights. Reliability Standard CIP-004-1R4 instructs the Responsible Entity to maintain "list(s) of personnel with authorized cyber or authorized unescorted access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets." Therefore, the CCA list utilized by TRE_URE2 was noncompliant. The remediated issue period was from the date the Standard was enforceable for TRE_URE2, to the date the revised list was implemented.	The issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because TRE_URE2 was consistently monitoring personnel electronic access rights and relied upon documented policies and procedures to manage personnel CCA electronic access rights. However, its monitoring efforts lacked sufficient documented detail regarding the scope of an employee's electronic access rights which had the potential to compromise BPS reliability in the event the original list alone was relied upon to grant electronic access. Further, the CCA access list is reviewed weekly in team meetings and necessary amendments are immediately documented by the meeting leader. Lastly, despite the lack of active list providing sufficient detail regarding specific electronic access rights, since TRE_URE2's registration, the same four employees (in a department of five) have managed electronic access authorizations and were familiar with the TRE_URE2's personnel and procedures. Based on these facts, Texas RE determined that the issue is primarily documentation related.	The violation remediated issue was fully mitigated with the implementation of the revised personnel CCA access list. The new list includes greater detail regarding more specific electronic access rights information. All mitigating activities have been verified as complete by Texas RE.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1) Duke Energy Generation Services, Inc. (DEGS)	NCRXXXXX	WECC2012011055	CIP-002-3	R4	WECC_URE1 submitted a Self-Report addressing an issue with CIP-002-3 R4. According to the Self-Report, during the calendar year 2010, WECC_URE1 failed to document annual approval of its risk-based assessment methodology (RBAM). Per CIP-002-3 R4, WECC_URE1 is required to keep a signed and dated record of the senior manager or delegate's annual approval of the RBAM, the list of Critical Assets (CAs) and the list of Critical Cyber Assets (CCAs). WECC_URE1 discovered that it did not have a signed and dated record of the then-senior manager's approval of the RBAM (the associated lists, however, had been approved, signed and dated). A WECC Subject Matter Expert (SME) reviewed the Self-Report and discussed the issue with WECC_URE1's compliance personnel. The SME determined that WECC_URE1 had identified and documented an RBAM to use to identify its CAs, and had developed a list of its identified CAs and associated CCAs, through an annual application of the RBAM. When WECC_URE1 applied the RBAM, it resulted in null lists because WECC_URE1 had no CAs or associated CCAs. These null lists had been reviewed and approved by the then senior manager. However, that senior manager did not sign and date a copy of the RBAM for 2010. The SME forwarded these findings to the WECC Enforcement Department (Enforcement). Enforcement reviewed the Self-Report and the auditors' findings, and determined that WECC_URE1 had an issue with CIP-002-3 R4, because it failed to have documentation that a senior manager or delegate approved the risk-based assessment methodology for 2010.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. WECC_URE1 did not have any CAs or CCAs. Although WECC_URE1's senior manager failed to sign the RBAM during calendar year 2010, he did sign and approve the null lists of CAs and CCAs.	WECC_URE1 remediated this issue. In April 2011, WECC_URE1 created a single point of contact, eliminated dual responsibility across its affiliated entities, and made one senior manager the delegate for all of its affiliated entities. The senior manager approved the RBAM for all WECC_URE1's registered entities.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012011027	CIP-007-3	R7	WECC_URE2 submitted a Self-Report citing an issue with CIP-007-3 R7. WECC_URE2 reported that it failed to follow its CIP-007-3 R7 procedure when disposing of a Critical Cyber Asset (CCA). WECC Subject Matter Experts (SMEs) reviewed WECC_URE2's Self-Report. SMEs contacted WECC_URE2 to request additional information. SMEs determined that one CCA associated with WECC_URE2 failed and could not be rebooted. WECC_URE2 staff usually assigned to handle CIP equipment failures were out of the office. The router was, therefore, removed by a technician who was not familiar with WECC_URE2's CIP-007-3 R7 disposal procedure. Instead of completing the decommissioning checklist required under WECC_URE2's CIP-007-3 R7 process, the technician followed the WECC_URE2 corporate cyber asset removal procedure and completed corporate documentation. The technician removed the router and sent the device back to the vendor without completing the CIP-007-3 R7 checklist necessary for CCA disposal. SMEs determined that WECC_URE2 had a possible issue with CIP-007-3 R7 and forwarded their findings to WECC Enforcement (Enforcement). Enforcement reviewed WECC_URE2's Self-Report and SMEs' findings. Enforcement determined that WECC_URE2's failure to follow CCA disposal procedures when decommissioning a CCA on May 21, 2012, constitutes an issue with CIP-007-3 R7.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system. The risk posed by WECC_URE2's failure is minimal because there were compensating measures in place. Although the WECC_URE2 technician did not complete the WECC_URE2 decommissioning checklist required under WECC_URE2's CIP-007-3 R7 process for CCA disposal, the technician did follow WECC_URE2 Corporate Policy regarding Cyber Asset disposal. The technician documented the device's failure and removal. The technician returned the device to the vendor. At the time of removal, the device would not reboot or power on, and the device was password protected. This minimized the risk of unauthorized retrieval of WECC_URE2's data, and the risk that the device could be used as an access point to the Electronic Security Perimeter. WECC_URE2 received confirmation from the vendor that the device was received and destroyed.	WECC_URE2 completed the following remediation activities: The device was destroyed. WECC_URE2 completed the CIP-007-3 R7 checklist required for device disposal. WECC_URE2 revised its CIP-007-3 R7 procedures to address a new decommissioning process to be followed for all devices. Further, as preventative measures, WECC_URE2 undertook training or retraining for any personnel that have access to any CIP network device on this new procedure.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201001975	CIP-002-1	R1	WECC_URE3 submitted a Self-Certification addressing its possible noncompliance with CIP-002-1 R1. Specifically, WECC_URE3 reported its status as "Beginning Work." The Audit Team determined WECC_URE3 did not have a documented RBAM until August 30, 2010, as WECC had previously alleged. The Audit Team also determined that the appropriate application of WECC_URE3's RBAM resulted in null lists for Critical Assests (CAs) and Critical Cyber Assets (CCAs) essential to the operation of a CA. On August 6, 2010, WECC found WECC_URE3 had an issue with CIP-002-1 R1 for failing to identify or document a Risk-Based Assessment Methodology (RBAM) to identify its Critical Assets as required by R1.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 applied its RBAM in 2011 and determined that it never had any CCAs essential to the operation of the CA. WECC subsequently verified this fact at an on-site Compliance Audit. Therefore, WECC determined WECC_URE3 does not have CCAs essential to the operation of the BPS. Moreover, the issues herein stem from WECC_URE3's failure to implement and document an RBAM for the period from December 31, 2009 to August 29, 2010. Because WECC_URE3 does not have CAs or CCAs, the BPS was never exposed or compromised by WECC_URE3's failure to comply with the documentation requirements of CIP-002-1 R1.	WECC_URE3 mitigated the issue with CIP-002-1 R1 by identifying and documenting its RBAM.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201001976	CIP-002-1	R2	WECC_URE3 submitted a Self-Certification addressing its possible issue with CIP-002-1 R2. Specifically, WECC_URE3 reported its status as "Beginning Work." WECC found WECC_URE3 had an issue with CIP-002-1 R2 for failing to develop a list of its identified Critical Assets (CAs) from the application of an RBAM as required by R2. The Audit Team determined WECC_URE3 did not have a documented RBAM until August 30, 2010. The Audit Team also determined that the appropriate application of WECC_URE3's RBAM resulted in null lists for CAs and Critical Cyber Assets (CCAs) essential to the operation of a CA.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 applied its RBAM in 2011 and determined that it never had any CAs or CCAs essential to the operation of the CA. WECC subsequently verified this in an on-site Compliance Audit. Therefore, WECC determined WECC_URE3 does not have CCAs essential to the operation of the BPS. Moreover, the issues herein stem from WECC_URE3's failure to implement and document an RBAM for the period from December 31, 2009 to August 29, 2010. Because WECC_URE3 does not have CAs or CCAs, WECC determined that the issues with CIP-002-1 R2 posed a minimal risk to the reliability of the BPS.	WECC_URE3 mitigated the issue with CIP-002-1 R2 by applying the RBAM developed in R1 to identify its CAs. As a result of this process, WECC_URE3 determined that it did not have any CAs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201001977	CIP-002-1	R4	WECC_URE3 submitted a Self-Certification addressing its possible issue with CIP-002-1 R4. Specifically, WECC_URE3 reported its status as "Beginning Work." WECC found that WECC_URE3 failed to have a list of Critical Assets (CAs) and a list of Critical Cyber Assets (CCAs) that were approved by a senior manager as required by R4. The Audit Team determined WECC_URE3 did not have a documented RBAM until August 30, 2010, as WECC had previously alleged. The Audit Team also determined that the appropriate application of WECC_URE3's RBAM resulted in null lists for CAs and CCAs essential to the operation of a CA.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 applied its RBAM in 2011 and determined that it did not have any CAs or CCAs essential to the operation of the CA. WECC subsequently verified this in an on-site Compliance Audit. Therefore, WECC determined WECC_URE3 does not have CCAs essential to the operation of the BPS. Moreover, the issues herein stem from WECC_URE3's failure to implement and document an RBAM for the period from December 31, 2009 to August 29, 2010.	WECC_URE3 mitigated the issue with CIP-002-1 R4 by providing a signed and dated record of the senior manager's approval of the null list of CAs and the null list of CCAs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2011008673	CIP-002-1	R3	As a result of a Compliance Audit, WECC found that WECC_URE3 had an issue with CIP-002-1 R3 for its failure to develop a list (albeit a null list) of associated Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset (CA). The Audit Team determined WECC_URE3 did not have a documented RBAM until August 30, 2010, as WECC had previously alleged. The Audit Team also determined that the appropriate application of WECC_URE3's RBAM resulted in null lists for CAs and CCAs essential to the operation of a CA.	This issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). WECC_URE3 applied its RBAM in 2011 and determined that it never had any CCAs essential to the operation of the CA. WECC subsequently verified this in an on-site Compliance Audit. Therefore, WECC determined WECC_URE3 does not have CCAs essential to the operation of the BPS. Moreover, the issues herein stem from WECC_URE3's failure to implement and document an RBAM for the period from December 31, 2009 to August 29, 2010.	WECC_URE3 mitigated the issue with CIP-002-1 R3, WECC_URE3 used the null list of CAs, and developed a subsequent null list of CCAs essential to the operation of the CAs.

Document Accession #: 20121130-5378 Filed Date: 11/30/2012

Document Content(s)