Federal Energy Regulatory Commission
Washington, D.C. 20426

January 4, 2022

FOIA No. FY19-30 (RC12-12)
Forty Fifth 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 23, 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. RC12-12, along with the names of eleven (11) 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 RC12-12.

[1] 5 U.S.C. § 552 (2018).

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

With respect to the remaining identities of UREs contained in RC12-12, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-12 will not be disclosed.

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

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

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2022.01.04 10:35:35 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

May 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. RC12-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 40 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 55 possible violations[5] of 19 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 55 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

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

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is 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, spot check, 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) Find Fix and Track Report 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 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 david.cook@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

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
david.cook@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

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

NERC

Attachment b

Additions to the service list

ATTACHMENT B

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

FOR FRCC:

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
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Director of Regulatory Affairs and Enforcement
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
(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:

R. Scott Henry*
President and CEO
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8202
(704) 357-7914 – facsimile
shenry@serc1.org

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

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*
Interim General Manager
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1730
(501) 821-8726 – facsimile
rciesiel.re@spp.org

Joe Gertsch*
Manager of Enforcement
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1672
(501) 821-8726 – facsimile
jgertsch.re@spp.org

Machelle Smith*
Paralegal & SPP RE File Clerk
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1681
(501) 821-8726 – 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

Sandy Mooy*
Associate General 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

Christopher Luras*
Manager of Compliance 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

NERC

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. RC12-___-000

NOTICE OF FILING
May 30, 2012

Take notice that on May 30, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding forty (40) 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)	Tampa Electric Company (TEC)	NCR00074	FRCC2012009108	BAL-004-0	R3	TEC, as a Balancing Authority (BA), self-reported that it identified two occurrences (on September 23, 2011 and November 9, 2011, respectively) where it did not participate in a Time Error Correction when requested to do so by the Reliability Coordinator.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). TEC's contribution to the Time Error Correction from a generator standpoint, relative to the Eastern Interconnection, is small at 1.7%. In each instance, TEC was generating to a slightly higher frequency. In addition, TEC met its Control Performance Standard (commonly known as CPS1 and CPS2) values and because TEC's contribution to the Eastern Interconnection Time Error Correction would have only been 0.00014 Hz, this would not be seen by the BAs in the Eastern Interconnection because the frequency increase is smaller than the 0.001 Hz accuracy requirement for the digital frequency monitor.	TEC completed the following mitigation activities: (1) Sent a reminder email from the manager of grid operations to electric system operators (ESOs), emphasizing the requirement to participate in Time Error Corrections; (2) Researched to determine if any additional Time Error Corrections were missed between January 1, 2011 and November 8, 2011 and found none besides the two issues described herein; (3) Modified the Time Error Correction documentation worksheet and provided spot training to ESOs on filling it out to capture information regarding each Time Error Correction; (4) Created a report in EA-Online database, which is a data repository visible to ESOs on an ongoing basis, such that they can monitor information and reports throughout their shift. Using EA-Online, the ESO can check the status of a scheduled Time Error Correction. This report helped ensure that a Time Error Correction is properly implemented in the Energy Management System; (5) Modified the Time Error Correction documentation worksheet to include checking the status in EA-Online; and (6) Reviewed the Time Error Correction requirement, BAL-004-0 R3, with ESOs during TEC's first quarter 2012 ESO training class.
Florida Reliability Coordinating Council, Inc. (FRCC)	Pinellas County Resource Recovery (PCRR)	NCR00060	FRCC2012009644	PRC-005-1	R2	PCRR, as a Generator Owner, self-reported that it identified two months (January 2011 and March 2011) where it could not find documentation or evidence of monthly battery testing as required by its PRC-005-1 maintenance and testing program.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the batteries are continuously monitored and would alarm the control room if any issues were identified. Additionally, the batteries were visually checked each day while operators were doing rounds, and documentation is lacking for only two months of monthly battery testing.	PCRR completed the following mitigation activities: (1) The preventative maintenance work order descriptions now have the words "FRCC Requirement" on them so they can be more easily identified and prioritized; and (2) A full-time employee of the operator is responsible for the tracking, reporting, and record-keeping relating to PRC-005. A new job description for the full-time employee was written, the employee was trained on the duties of the position, and has acknowledged the training.
Midwest Reliability Organization (MRO)	Dairyland Power Cooperative (DPC)	NCR00979	MRO201100318	VAR-002-1.1b	R3	During a regularly scheduled compliance audit, conducted between March 7, 2011 through March 11, 2011, MRO discovered that DPC, registered as a Generator Operator (GOP), failed to notify its Transmission Operator (TOP) within 30 minutes of the status change of an automatic voltage regulator (AVR). On December 13, 2010, DPC removed a unit named "JPM" from service. Per the DPC voltage schedule, once the JPM unit comes off line, two other units, Alma 4 and Alma 5, if in service, must place their AVRs in service. MRO requested records evidencing that the AVRs were placed in service. DPC reviewed its TOP logs but could not identify whether the AVRs were placed in service. MRO then requested documentation for the Alma station alarm summary, Alma operator logs, the TOP logs, and the voice recordings for this event. DPC provided the Alma station alarm summary which included evidence indicating the AVRs were placed in service. However, neither the Alma station log nor the TOP log included documentation indicating that the GOP notified the TOP of the change of AVR status. The voice recorder for the TOP was out of service during the week of the event. Therefore, without supporting documentation or corroborating voice recordings, DPC was unable to verify that the TOP was notified within 30 minutes of the status change of the AVR.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because DPC's Energy Management System (EMS) provides a continuous indication of the AVR status to the TOP, and DPC provided both station alarms and operator logs to prove that the changes were made within 30 minutes as required in VAR-002. DPC provided evidence from its control system alarm log that the AVRs were indeed placed in-service as per the plan and DPC stated that it notified the TOP through a phone conversation although DPC's voice recording system did not have a record of the conversation.	DPC performed the following actions to mitigate the issue: (1) verified that primary and back-up voice recording systems were in working order; (2) updated the DPC voltage and reactive criteria; (3) trained staff on the updated procedures; (4) performed an internal spot check on AVR status change and communication logs; and (5) tested the AVR alarm through the EMS for JPM.
Northeast Power Coordinating Council, Inc. (NPCC)	First Wind O&M, LLC (FW O&M)	NCR10331	NPCC2011009013	PRC-005-1	R1	On November 8, 2011, FW O&M, as a Generator Owner (GO), self-reported to NPCC an issue with PRC-005-1 R1. FW O&M reported that they did not have a Protection System maintenance program for two generating assets, Stetson I and Stetson II. A Protection System maintenance and testing program was implemented on March 3, 2010, 18 days after these units were registered with NPCC on February 13, 2010.	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 FW O&M did not have a formalized maintenance and testing program in place prior to registering as a GO, the program was issued 18 days after registration and prior to the actual commercial operation of Stetson II. In addition, Stetson I and II were constructed in 2008 and all Protection Systems were tested during commissioning.	FW O&M completed mitigation activities by approving and implementing its Protection System maintenance and testing procedure for Stetson I and II. The mitigation activity was verified complete by NPCC.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	First Wind O&M, LLC (FW O&M)	NCR10331	NPCC2011009014	PRC-005-1	R2	On November 8, 2011, FW O&M, as a Generator Owner, self-reported to NPCC an issue with PRC-005-1 R2. FW O&M reported that during an internal audit, it was discovered that testing at the Stetson I and Stetson II substations had not been performed in accordance with the intervals defined in the Stetson I/Stetson II Protection System maintenance and testing program. The program calls for data verification testing and voltage and current inputs of the Protection System equipment to be performed every six months. FW O&M failed to complete this testing for two six-month testing intervals. The first testing should have taken place in September 2010 and the second testing in March 2011. The actual testing was completed on September 13, 2011.	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 FW O&M took immediate action upon discovery and completed the series of testing as per its system maintenance and testing procedure in September 2011. Also, although FW O&M did not complete testing in accordance with the intervals defined in the Stetson I/Stetson II Protection System maintenance and testing program, its program is robust in that its testing intervals exceed those specified by the NERC-published document *Protection System Maintenance - A Technical Reference* (September 13, 2007).	FW O&M completed mitigation activities by completing the required testing in accordance with the testing interval requirements of the Stetson I/Stetson II Protection System maintenance and testing program. Additionally, FW O&M took action to review its existing program and reinforce the requirements of PRC-005 with responsible site personnel. Also, FW O&M assigned the reliability and compliance manager the responsibility to review future test dates with responsible personnel and confirm that testing is scheduled and conducted at intervals specified in the Stetson I/Stetson II Protection System maintenance and testing program. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	New Athens Generating Company, LLC (Athens)	NCR07154	NPCC2011007567	PRC-005-1	R2	On June 17, 2011, Athens, as a Generator Owner, self-reported to NPCC an issue with PRC-005-1 R2. During a scheduled review of the Athens generation Protection System maintenance and testing program, it was determined that certain relay testing associated with unit 2 had not been performed in accordance with the established interval schedule. Testing was scheduled prior to summer 2011. In January 2011, Athens unit 1 main transformer experienced a major failure and was not expected to return to service until August 2011. In an effort to maintain grid support during the summer period, a decision was made to delay the unit 2 outage, preventing testing of the relays within the required time interval. The relays not tested comprised 30% of the total number of relays subject to 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 (BPS) because although testing was not completed within Athens's established testing interval, testing was completed in September 2011, less than four months late, according to the established testing interval. Also, the interval for Athens's relay testing is a two-year cycle, which is shorter than the interval specified by the NERC-published document *Protection System Maintenance - A Technical Reference* (September 13, 2007). The decision to delay testing was the result of an effort to maintain grid support and reliability during the summer period, which is the peak load period for the New York region.	Athens completed mitigation activities by: (1) Performing relay testing as required; and (2) Modifying tasks in its maintenance management system to add clarity to testing requirements and intervals and to assign due dates 90 days prior to the actual due dates. The mitigation activity was verified complete by NPCC.
SERC Reliability Corporation (SERC)	City of Columbia, MO (CWLD)	NCR01196	SERC201000630	FAC-008-1	R1	On September 30, 2010, CWLD, as a Transmission Owner, self-reported an issue with FAC-008-1 R1 because its Facility Rating Methodology (FRM) did not address current transformers (CTs) integrated into circuit breakers. SERC staff learned that, in preparation for a SERC Audit scheduled for October 2010, CWLD contracted with an independent external auditor to perform an internal audit in early September 2010. This audit revealed that the FRM did not address CTs integrated into circuit breakers (integral CTs). SERC staff reviewed the version of the FRM in effect at the time of the Self-Report. SERC staff confirmed that the FRM addressed transmission conductors, transformers, relay protective devices, and terminal equipment including free-standing CTs, but it did not address integral CTs. SERC staff also noted that CWLD's FRM addressed series compensation devices, stating that it had none, but it did not address shunt compensation devices. SERC staff also reviewed two previous versions of CWLD's FRM, neither of which addressed integral CTs or shunt compensation devices.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Although CWLD failed to include shunt compensation devices in its FRM, it has never owned shunt compensation devices and they would not have been a limiting device; 2. After CWLD factored integral CTs into its Facility Ratings, CWLD decreased the Facility Ratings for two transmission facilities and one distribution facility, each by less than 10% of the original Facility Rating. CWLD's subsequent contingency analysis found that the decreased ratings were not sufficient to warrant changes to transmission plans or to affect daily grid operations; and 3. CWLD is a small system with a 327 MW peak load and 30 miles of 161kV transmission line that serves as a high voltage distribution system for internal CWLD use and does not carry BPS networked energy transfers.	SERC staff verified that CWLD completed the following actions: 1. CWLD revised its FRM to include provisions for integral CTs and to indicate that CLWD does not own or operate shunt compensation devices; and 2. CWLD re-rated its facilities and performed an assessment with the corrected ratings to ensure that Bulk Electric System performance continued to adhere to the requirements of the Transmission Planning Standards.
SERC Reliability Corporation (SERC)	Ameren Energy Resources (AER)	NCR10309	SERC201000562	VAR-002-1.1a	R3	On June 25, 2010, AER, as a Generator Operator, self-reported an issue with VAR-002-1.1a R3 after discovering that it had placed the power system stabilizer (PSS) for Unit #2 at its Newton generating facility in service without notifying the Transmission Operator (TOP) within 30 minutes. The Newton generating facility has two units, which each have a gross capacity of 686 MVA. On May 31, 2010, at approximately 9:00 p.m., AER brought Unit #2 on-line following an outage for boiler cleaning. AER's standard protocol is to operate the unit with the PSS in service. At approximately 2:00 a.m. on June 1, 2010, Unit #2 reached dispatchable load, at which time the operator should have placed the PSS in service. On June 4, 2010, the Shift Supervisor discovered that the PSS had not been placed in service and directed the Plant Operator to place the PSS in service. The Plant Operator placed the PSS in service at approximately 2:00 a.m., but failed to notify the TOP within 30 minutes of the change in status of the PSS, as required. AER notified the TOP of the change in status on June 14, 2010.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. The Newton Unit #1 was online with the PSS in-service; and 2. Both Newton Units (#1 and #2) had the automatic voltage regulator (AVR) in service, which was regulating voltage at the time of the issue. By putting the PSS in service in this situation AER reduced the risk to the BPS. SERC determined that FFT treatment is appropriate in this case because of the mitigation measures implemented by AER and the minimal level of risk of the underlying issue.	AER has completed the following actions: 1. AER added automated eLog and e-mail notifications in order to alert the Plant Operator at Newton that the PSS status has changed. The automatic notification includes a note to notify the TOP within 30 minutes; 2. The e-mail notifications will also be sent to the Plant Superintendent and Plant Manager at Newton; 3. Newton has added the PSS to the Newton startup checklist to be verified during initial plant startup; and 4. For other AER units with PSS, their startup check lists were reviewed to verify inclusion of the PSS status and revised where necessary.

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)	Associated Electric Cooperative, Inc. (AECI)	NCR01177	SERC201000600	PRC-005-1	R2	On August 18, 2010, AECI, as a Generator Owner and Transmission Owner, self-reported an issue with PRC-005-1 R2 after it discovered that generating stations Unit 1 and 2 at its St. Francis plant did not have data to prove that testing of the voltage and current sensing devices (instrument transformers) had been completed within the six-year period stated in AECI's maintenance and testing program. AECI performed a complete review of all 109 transmission substations 100 kV and above to ensure that a current test for each element with the transmission Protection System was available and that there was sufficient evidence to show that a previous test was performed within the time intervals stated in AECI's maintenance and testing program. On August 26, 2010, AECI self-reported another possible issue with PRC-005-1 R2 after it discovered that the Morgan 161 kV substation relays were trip tested outside of the time interval provided in the AECI transmission procedure and 44 days after the six month grace period expired. SERC staff determined that AECI tested 28 voltage and current sensing devices and five DC control circuitry devices outside of interval. Out of a total of 9,807 Protection System devices, AECI tested 33 devices (or 0.34%) outside of their defined intervals.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. AECI did not miss any required maintenance of its Protection System devices, such as replacing worn parts and calibrating the devices; 2. AECI noted that its St. Francis plant has a total rating of 614 MW, or 11.7% of AECI's total capacity of 5,255 MW, suggesting that any problems resulting from AECI's failure to test the Protection System devices at that location would likely have a small impact on AECI and the BPS as a whole; and 3. Additionally, AECI tested the Protection System devices at a later date and found all the devices were operating normally and did not require recalibration.	SERC staff verified that AECI completed the following actions: 1. AECI, upon discovery of the issue, immediately tested the voltage and current sensing devices at St. Francis Unit 1 and 2; 2. AECI has implemented all of the Protection System elements within the Generator Plants associated with NERC standard PRC-005 to its task-based software tool used by the plants to track and verify maintenance; 3. AECI has added an alarm within its compliance tracking software to review its records associated with NERC relay maintenance and testing twice per year; 4. AECI has reviewed of all its transmission substations associated with PRC-005 to ensure that they are in compliance with the Standard; and 5. AECI has implemented a requirement to review all substation testing once per quarter to ensure that the required intervals are being met. AECI added this requirement to its compliance tracking software as an alarm to its personnel once per quarter.
SERC Reliability Corporation (SERC)	Louisiana Generating, LLC (LaGen)	NCR01265	SERC2011007979	BAL-005-0.1b	R17	On September 1, 2011, LaGen, as a Balancing Authority (BA), self-reported an issue with BAL-005-0.1b R17, stating that one of its frequency sources did not specify the required accuracy of less than or equal to 0.001 Hz. SERC staff learned that, at the start of 2011, LaGen incorporated the City of Conway (Conway) BA into LaGen's Balancing Area. In preparation for the cutover, LaGen had installed metering and monitoring equipment on the Conway tie line, including a frequency transducer for telecommunication of the frequency on the tie line from Conway to LaGen. LaGen's Energy Management System uses the telemetered information in the display of data for the operators and in the calculation of the Area Control Error for the Conway BA. SERC staff learned that the Conway Remote Terminal Unit was not properly calibrated, resulting in the frequency source being calibrated to an accuracy of 0.01 Hz. SERC staff confirmed that the frequency monitor was calibrated at 60.00 Hz and had not been calibrated to the required three digit accuracy.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. Based on LaGen's calculations using the maximum possible error that the frequency monitor could have introduced, the inaccuracy introduced a maximum of 0.2 MW into the ACE calculation; and 2. During the seven months the inaccurate data was being used, LaGen's Control Performance Standard 1 (CPS1) calculations were all within the compliant range, indicating that the issue had a minimal effect on LaGen's ability to adequately monitor and control generation.	SERC staff verified that LaGen completed the following actions: 1. LaGen changed the miscalibrated frequency source to another source with a confirmed three decimal calibration; 2. LaGen's parent company has reviewed its affiliated BAs to ensure that a similar situation does not exist elsewhere; and 3. To ensure this does not happen in the future, LaGen's parent company has: a. Installed a new primary frequency source at Conway; b. Revised its BA Operations Document, BAL-005, to include additional departments and a statement for R17 to direct the target audience to other related documents specific to each individual BA. c. Revised the Telecommunications Detail documents for LaGen and the Conway, City of West Memphis, and City of North Little Rock, AR BAs, which have been incorporated into LaGen's BA, to include more detail on the frequency sources used for BAL-005 and the NERC requirements for accuracy.

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)	Louisiana Generating, LLC (LaGen)	NCR01265	SERC201100746	BAL-005-0.1b	R12	On January 7, 2011, LaGen, as a Balancing Authority (BA), self-reported an issue with BAL-005-0.1b, stating that it discovered that two new Tie Line flows were modeled in LaGen's Energy Management System (EMS) but not activated in the Area Control Error (ACE) calculation. SERC staff confirmed that LaGen had established one Tie Line each to two BAs that were not previously included in LaGen's BA Area. The two new Tie Line flows were modeled and incorporated into the LaGen EMS on January 1, 2011. After the cutover included the new Tie Lines, LaGen checked the systems and found that the EMS was capturing the revised Tie Line data, and LaGen assumed that the cutover had been successful. As time passed, however, LaGen operators noted an increase in Inadvertent Interchange, prompting LaGen personnel to investigate the cause. LaGen discovered that although the two new Tie Line flows to the adjacent BA Areas were properly accounted for in the EMS, they were not properly accounted for in the ACE calculation for Automatic Generation Control (AGC). LaGen determined that its technician who implemented the new model had not reset the Tie Line record field in the AGC to include the two new Tie Lines in the ACE calculation. As a result, the AGC did not receive data indicating the power flow on the new Tie Lines and did not adjust generation as those flows changed. According to LaGen's recorded data, in the hours immediately following the cutover the total Tie Line flows were less than 10 MW on a system balancing over 1,300 MW. In the first 24 hours after the cutover, of the 35,184 MW that were accounted for in the EMS, 763 MW (roughly 2%) were not included in the ACE calculation used for AGC. Due to this small error, LaGen personnel did not notice the failure to include the metered values until the loads were increased without a corresponding change in ACE and the increase in Inadvertent Interchange could not be explained.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The combined Tie Line flows that were not included in the ACE calculation were a small contribution (approximately 2% of the total MW over 24 hours accounted for in the EMS) to the flows being managed by LaGen and would have had a similarly small contribution to the AGC if they had been included in ACE calculation; and 2. The issue duration was fewer than 4 days.	SERC staff verified that LaGen completed the following actions: 1. LaGen corrected the two Tie Line Record fields, which added them to the LaGen ACE calculation; and 2. To ensure this does not happen in the future, LaGen's parent company has: a. Implemented a new procedure for its BA Operators to verify ACE; b. Revised the BA cutover procedure for the EMS support team to ensure Tie Lines added to the EMS are properly accounted for in the ACE calculation, including procedures to guide the programmer that describe how to add a Tie Line in the EMS and a method for verifying that the LaGen ACE calculation is correct; c. Developed a new tool to compare the average interchange component of ACE with hourly inadvertent with a threshold to initiate an alarm to the EMS, BA Operators, and LaGen System Operators. A procedure has also been created to explain the process and expectations of the parties involved; and d. Created a separate calculation for BA ACE, which is used to compare it to the EMS AGC ACE calculation, and alarm and email responsible personnel upon deviation from a programmable threshold.
SERC Reliability Corporation (SERC)	Louisiana Generating, LLC (LaGen)	NCR01265	SERC201000509	FAC-008-1	R1	On March 26, 2010, the SERC audit team reported an issue with FAC-008-1 R1, stating that there was a document-only gap for LaGen's Generator Owner (GO) function and that LaGen did not have an established Facility Ratings Methodology (FRM) for generation facilities between June 18, 2007 and December 31, 2008. SERC staff reviewed LaGen's FRM for the GO function, which comprises two FRM documents, one from 2008 and the other from 2009. The 2008 FRM document failed to address series and shunt compensation devices and failed to consider equipment manufacturers' ratings, design criteria, ambient conditions, operating limitations or other assumptions. The 2009 FRM document considered equipment manufacturers' ratings, design criteria, ambient conditions, operating limitations and other assumptions, but failed to address series and shunt compensation devices for the generation facilities. SERC staff also reviewed LaGen's FRMs for the Transmission Owner function and had no findings of non-compliance.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. LaGen's 2009 FRM addressed the requirements of FAC-008 with the exception of series and shunt compensation devices; 2. Although LaGen's generation FRM documents failed to include series or shunt compensation devices, LaGen does not own series or shunt compensation devices for its generation assets; 3. LaGen's 2007 Facility Rating did not change in LaGen's 2008 FRM, both of which identified the most limiting element as the generator; and 4. In May 2007, LaGen provided all generation and transmission bus data to its transmission providers for distribution to the appropriate planning personnel. As a result, LaGen's generation and transmission bus data has been available to the transmission providers for use in the transmission providers' models and studies.	SERC staff verified that LaGen completed the following actions: LaGen produced a companion document to its parent company's corporate document addressing facility ratings, methodology, and communication for the Generating plants in December 2008, and LaGen's January 2012 Power Plants FRM lists equipment to be accounted for in its FRM where applicable and includes series and shunt compensation devices.

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)	Mid Georgia Cogen L.P. (MidGa)	NCR00167	SERC2011007446	TOP-002-2	R18	On June 17, 2011, the SERC audit team reported an issue with TOP-002-2 R18, stating that MidGa, as a Generator Operator, was unable to demonstrate that transmission line and equipment identifiers used by MidGa were uniform with the identifiers used by the interconnected Transmission Operator, Georgia Power Company (GPC). GPC owns and operates the Substation adjacent to the MidGa generating facility. The GPC Substation is where the switches are located and the line is connected. When the MidGa plant was originally interconnected with GPC, the interconnection used a tap of the Bonaire to Pitts 230 kV line. In 2001, GPC installed the Kathleen Substation to take the place of the simple tap point and updated its one-line diagram to reflect this change. MidGa did not update its one-line diagram and still listed the tie-point as the Bonaire to Pitts 230 kV line. In addition, MidGa's one-line diagram did not contain the switch numbers to match the GPC one-line diagram. SERC staff reviewed the MidGa and GPC one-line diagrams and confirmed the audit team's findings that MidGa failed to update its one-line diagram to show the connection via the Kathleen Substation and failed to include switch numbers that matched GPC's one-line diagram. SERC staff also determined that MidGa's one-line diagram did not contain the breaker number that was used in GPC's one-line diagram.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. MidGa management was aware of the GPC numbers for the switches but they were not aware that they needed to be included on the MidGa one-line diagram; 2. GPC manages the transmission line and Substation at the MidGa facility where the companies' facilities interconnect; 3. When outages are necessary, they are coordinated between GPC and MidGa. GPC clears the lines on site at its Substation, which includes a visual inspection of the clearances and, when allowed, the installation of its locks on the switches as part of the clearance. This coordinated outage process has been used since the completion of MidGa's plant in 1998. Since employees of both companies are present to perform clearances, there is a reduced chance of operating the wrong devices, and the disconnect switches that MidGa failed to label are only operated for electrical maintenance; 4. MidGa had performed clearances correctly despite the fact that its one-line diagram did not reflect the proper naming and numbering used in GPC's one-line diagram; and 5. If a switch ever misoperated, it would only impact the MidGa facility because the MidGa facility is radially connected to the bulk power system through GPC.	SERC staff verified that MidGa completed the following actions: 1. MidGa updated its one-line diagram to match GPC's one-line diagram; and 2. Going forward, MidGa will make an annual request to GPC to ensure that MidGa receives the latest revision of GPC's one-line diagram.
SERC Reliability Corporation (SERC)	Nelson Industrial Steam Company (NISCO)	NCR09017	SERC2011007535	IRO-004-1	R4	On June 28, 2011, NISCO, as a Generator Owner, self-reported an issue with IRO-004-1 R4, stating that it failed to provide information required for system studies, such as critical facility status and generation, by 1200 Central Standard Time (for the Eastern Interconnection). The Nelson site has two generation units owned by NISCO and several other generation units owned by Entergy. Entergy operates all of the generation units at the Nelson site, including the two NISCO units. NISCO depended on local Entergy personnel to make the necessary communications for the two NISCO units. Entergy personnel at the Nelson site communicated NISCO's planned outage information and daily forecasted generation information to Entergy's Entergy Management Organization (EMO)/System Planning and Operations (SPO) Group. Both NISCO and local Entergy personnel thought the EMO/SPO Group communicated all of the information about the NISCO units to the Transmission Operator (TOP). A procedure upgrade initiated by NISCO prompted NISCO and local Entergy personnel to follow up with the EMO/SPO Group, at which point NISCO learned that the EMO/SPO Group was communicating planned outage information, but not daily forecasted generation information, to the TOP. NISCO immediately contacted the TOP, which directed NISCO to a procedure on how to report daily generation information, including scheduled generator outages and expected generation profiles, to the TOP and the Reliability Coordinator. SERC staff confirmed that NISCO sent its generation information for May 7, 2011 to the correct email address stated in the TOP procedure and that the TOP started receiving the required information on May 7, 2011.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. Although daily forecasted generation information was not reported to the TOP, NISCO's planned outage information was communicated to the TOP; and 2. NISCO's ability to impact the Balancing Authority's area is minimal because its 200 MW is approximately 0.7% of the 30,000 MW total generation available.	SERC staff verified that NISCO completed the following actions: 1. Immediately after discovering that daily load projections were not being communicated to the TOP as required, NISCO personnel communicated and coordinated with the TOP to facilitate the communication of daily load capability as desired by the TOP; and 2. NISCO personnel have completed the development and implementation of a new procedure that addresses compliance with IRO-004-1 R4 and includes specific guidelines and communication methodology to prevent any future potential issues with IRO-004-1 R4.

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)	Nelson Industrial Steam Company (NISCO)	NCR09017	SERC2012009693	PRC-005-1	R1	On February 9, 2012, NISCO, as a Generator Owner, self-reported an issue with PRC-005-1 R1, stating that it did not adequately document the interval basis or the summary of the maintenance and testing procedures for batteries. SERC staff requested NISCO's protection system maintenance and testing program and all supporting documentation since June 28, 2007. SERC staff reviewed the program and procedures and determined that NISCO did not have a documented battery maintenance and testing program that included intervals, interval basis, and a summary of maintenance and testing procedures prior to June 2, 2009. SERC staff also confirmed that NISCO's maintenance and testing program covered protective relays, voltage and current sensing devices, and DC control circuitry during the period of the issue. NISCO's maintenance and testing program states that NISCO does not own any associated communication devices, which SERC confirmed.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. NISCO performed maintenance and testing on batteries according to the Generator Operator's (GOP) automated maintenance management system, which issued a preventative maintenance document monthly with the maintenance information to perform battery maintenance; and 2. NISCO has used the GOP's maintenance management system since June 2007.	SERC staff verified that NISCO completed the following actions: 1. In June 2009, NISCO began using a new procedure developed by the Generator Operator (GOP) for battery maintenance and testing; 2. NISCO further developed its own battery maintenance and testing procedures to be used along with the GOP procedures. NISCO revised its generator relay maintenance and testing program procedures to address the maintenance and testing intervals and the summary of maintenance and testing procedures to better ensure compliance with the PRC-005 standard; and 3. In 2011, NISCO also developed its own preventive maintenance basis document to be used in conjunction with the GOP procedures.
SERC Reliability Corporation (SERC)	Nelson Industrial Steam Company (NISCO)	NCR09017	SERC2011008093	PRC-005-1	R2	On September 19, 2011, NISCO, as a Generator Owner, self-reported an issue with PRC-005-1 R2, stating that it could not produce evidence that battery maintenance activities had been performed in accordance with its maintenance and testing program. NISCO could not find evidence that the battery had been tested monthly in January, May, and November of 2008, and February and May of 2009. SERC staff requested and reviewed a spreadsheet that included each of NISCO's Protection System devices and the defined maintenance and testing intervals, the most recent test date, and the previous test date for each device. SERC staff verified the defined intervals were the same in the spreadsheet and in NISCO's PRC-005 maintenance and testing procedures. SERC staff determined that NISCO could not provide evidence that one of its 125 Protection System devices (or 0.8%) was tested within the defined intervals.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. For all five instances of the missed monthly test, NISCO tested the battery the month following the missed interval; 2. NISCO's subsequent testing of the battery, including a capacity test, was successful and found no problems, suggesting that the battery likely would have performed as intended if called upon to do so; 3. NISCO personnel walk through the plant daily and conduct daily checks of the malfunction light on the battery charger; and, 4. NISCO was able to provide evidence of maintenance and testing records for 99% of its Protection System devices.	SERC staff verified that NISCO completed the following actions: 1. NISCO has implemented a comprehensive maintenance scheduling, implementation and documentation tracking system to facilitate rigorous oversight of contractor maintenance activities; 2. This system will enable management personnel to ensure that scheduled maintenance activities are completed within scheduled time frames and required, acceptable documentation is provided to management personnel in a timely manner upon completion of scheduled maintenance activities; 3. NISCO has loaded all the maintenance activities into the maintenance tracking system and NISCO management receives an action item when maintenance items are scheduled, thereby allowing NISCO to monitor the maintenance program independent of the maintenance contractor's program; and 4. Each action item requires that the preventive maintenance data be given to NISCO for review. The action item is closed following that review with the preventive maintenance data attached as evidence of the completion of the item.
SERC Reliability Corporation (SERC)	Owensboro, KY Municipal Utilities (OMU)	NCR01290	SERC201000634	VAR-002-1.1a	R2	On September 30, 2010, OMU, as a Generator Operator, self-reported an issue with VAR-002-1.1a R2, stating it discovered occurrences of operation outside of the voltage schedule specified by the Transmission Operator (TOP). OMU operates a single generating facility. The facility consists of 2 units totaling approximately 400 MW. At the time of the issue, the TOP-provided voltage schedule was 141 kV with a bandwidth of +/– 1 kV. In preparation for its October 2010 Self-Certifications, OMU reviewed meter data and discovered that readings from its 138 kV bus showed voltage excursions outside of the TOP-provided voltage schedule. OMU reviewed data from August 1, 2009 through October 1, 2010 and reported that it experienced 26 excursions that were greater than 1% outside the voltage schedule. None of the excursions during that period were greater than 2% outside of the voltage schedule. The deviations from the voltage schedule ranged from –2.33 kV to +1.75 kV. During this time, OMU did not have an exemption from the TOP, and the TOP did not contact OMU to express its concern about OMU's deviations from the voltage schedule.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. OMU was regulating voltage to within approximately 1.6% of the TOP directed voltage schedule; 2. OMU worked with its TOP after identifying the issue to modify its voltage schedule, which the TOP expanded from the original 140 kV – 142 kV voltage schedule to 139 kV – 143 kV; and 3. The TOP did not contact OMU to express concern about OMU's deviations from the voltage schedule.	SERC staff verified that OMU completed the following actions: 1. Upgraded all meters at the plant, allowing OMU's control center and the Elmer Smith Station control room to utilize the same voltage source for control and indication; 2. Added voltage alarms in the plant control room, with both low and high alarms to indicate a deviation from the voltage schedule target and a "low low" and "high high" alarm to indicate that the voltage is at the lower or upper limit of the voltage schedule; 3. Enhanced plant operator's voltage display on each unit's master distributed control system screen so that it is always visible to the operator. A visual alarm state is also always visible to the plant operator; 4. Revised its current steady-state power flow model to evaluate voltage bandwidths of +/- 1.0 kV, +/- 1.5 kV, and +/- 2.0 kV at various system conditions to identify any adverse impacts; 5. Developed a revised Elmer Smith Station voltage schedule to incorporate the results of the Elmer Smith Station Voltage Set-point Study;. 6. Completed review by neighboring TOPs of the revised Elmer Smith Station voltage schedule; 7. Implemented the revised Elmer Smith voltage schedule; and 8. Conducted supplemental training for generator and transmission operators on the new voltage schedule and VAR-002-1.1a compliance issues.

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)	Progress Energy Carolinas (PEC)	NCR01298	SERC2012009652	BAL-004-0	R3	PEC self-reported an issue with BAL-004-0 R3.1 stating that PEC, as a Balancing Authority (BA), failed to participate in a Time Error Correction. SERC staff learned that, on December 13, 2011, the Eastern Interconnection's Interconnection Time Monitor (ITM) identified a need for a Time Error Correction and posted a message to the Reliability Coordinator Information System (RCIS) announcing the start of a Time Error Correction. The Reliability Coordinator (RC) also sent the message in an email to PEC. The end time of the Time Error Correction was scheduled to be the same day at 23:59 EST. At 22:45 EST on December 13, 2011, the ITM observed that the time error had been substantially reduced and posted a message to the RCIS announcing the end of the Time Error Correction at 00:00 EST on December 14, 2011. The RC subsequently emailed the same message to PEC. It was at this time that PEC identified its failure to participate in the Time Error Correction. SERC staff requested that PEC review its records to determine if it failed to participate in any other Time Error Corrections during the calendar year. PEC reviewed its logs and determined it participated in 51 Time Error Corrections in 2011. PEC reported that the RC's records indicate there were 52 Time Error Corrections performed during the 2011 calendar year, demonstrating that PEC only failed to participate in the December 13, 2011 Time Error Correction.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The December 13, 2011 Time Error Correction was successful; 2. PEC participated in 51 out of 52 Time Error Corrections in 2011; and 3. If the Time Error Correction had not been successful within the projected timeframe, the ITM could have extended the duration of, or reinitiated, the Time Error Correction.	SERC staff verified that PEC completed the following actions: 1. PEC reactivated the audible alarm on the RCIS; 2. PEC provided the RC with an updated email distribution list to ensure that all PEC system operators receive distribution list emails from the RC; 3. PEC revised its control room procedure for implementation of Time Error Corrections. The revised procedure establishes a primary role (Transmission Reliability Desk) and secondary role (the on-shift Supervisor) with specific Time Error Correction responsibilities. It requires RCIS audible alarms to be activated. It requires any individual that acknowledges an RCIS Time Error Correction notification to immediately notify the AGC Desk operator. The AGC Desk operator is then responsible for implementing the Time Error Correction and logging its implementation time; and 4. PEC obtained a second and separate RCIS account that is in use in the control room so that both the primary and secondary personnel have access to RCIS Time Error Correction notifications at their individual work stations.
SERC Reliability Corporation (SERC)	Tennessee Valley Authority (TVA)	NCR01151	SERC2011008005	INT-006-3	R1	On September 13, 2011, TVA, as a Balancing Authority (BA) and Transmission Service Provider (TSP), self-reported that on four separate occasions it was unable to take the required action in response to curtailment requests within the 10 minute period specified by the Standard's timing requirements table due to computer or system malfunctions. SERC staff learned that TVA utilizes a software application to manage Requests for Interchange (RFI). When a RFI is submitted for the next hour, the Standard's timing requirements table requires BAs and TSPs to respond to the RFI within 10 minutes. TVA was unable to take the required action within the 10 minute period due to malfunctions with the software application it uses to manage RFIs on the following occasions: 1. On January 2, 2011, the application had a refresh issue that lasted 3 hours, resulting in 12 requests for hourly tag curtailments totaling 18 MW automatically expiring; 2. On May 2, 2011, the application froze for less than 1 hour, resulting in 4 requests for hourly tag curtailments totaling 43 MW automatically expiring; 3. On June 12, 2011, the application froze for less than 1 hour, resulting in 1 request for a 50 MW hourly tag curtailment automatically expiring; and 4. On July 20, 2011, the application froze for less than 1 hour, resulting in 1 request for a 1 MW hourly tag curtailment automatically expiring. TVA queried its software database and reported that from January 2011 through July 2011, it processed a total of 3,258 tag curtailment requests. As part of its investigation into the cause of the issues, TVA contacted the software developer for the application TVA uses to manage RFIs. The software developer acknowledged that refresh issues had been reported for the version TVA had been using since September 1, 2010. TVA later updated the software application, which resolved the problem.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. From January 2011 through July 2011, TVA did not respond to only 18 out of 3,258 hourly tag curtailment requests; 2. The duration of TVA's failures to respond totaled fewer than 6 hours; and 3. Given the size of the curtailment requests, the failure of TVA to respond did not preclude relief from other means, including the use of spinning reserves or reserve sharing.	SERC staff verified that TVA completed the following actions: 1. Upgraded its software application which included alarming for critical processes; 2. Upgraded the computer hardware and operating system; and 3. Increased network bandwidth.

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)	Town of Sharpsburg (Sharpsburg)	NCR01348	SERC2011008218	PRC-008-0	R1	On September 22, 2011, Sharpsburg, as a Distribution Provider (DP), self-reported an issue with PRC-008-0 R1, stating that it did not have a documented underfrequency load shedding (UFLS) testing program prior to March 2011. SERC staff requested copies of Sharpsburg's UFLS procedures and other information necessary to complete its assessment. Sharpsburg's consultant sent underfrequency relay test results from March 11, 2008 and March 9, 2011. The test results list the one and only UFLS relay that Sharpsburg owns. Neither test result report provided a schedule for the next test date. Sharpsburg did note in its subsequent self-certifications, however, that the testing and maintenance would be done every three years. Shortly after its consultant attended a SERC open forum in which the documentation requirements for a UFLS equipment maintenance program were discussed, Sharpsburg developed an underfrequency relay testing and maintenance procedure, dated March 11, 2011. This procedure identifies Sharpsburg's one UFLS relay and calls for a three year equipment maintenance and testing schedule.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Although it lacked a documented UFLS program until March 11, 2011, Sharpsburg was testing the UFLS relay; and 2. Sharpsburg is a small utility with 4.8 MW of peak load and does not own any BPS facilities. Sharpsburg's contribution to underfrequency load shed pursuant to the SERC regional criteria (30% of peak load) is only 1.44 MW.	SERC staff verified that Sharpsburg completed the following actions: Sharpsburg developed a detailed UFLS testing procedure that provides the following information about its UFLS relay - its exact location; identification information, including the manufacturer, model, and serial number; the date by which the next testing will occur; and the testing and maintenance intervals.
Southwest Power Pool Regional Entity (SPP RE)	Louisiana Energy & Power Authority (LEPA)	NCR01116	SPP2011008479	EOP-008-0	R1.5; R1.6	During an October 18, 2010 through October 20, 2011 Compliance Audit, SPP RE determined that LEPA, as a Balancing Authority (BA), was noncompliant with EOP-008-0 R1.5 and R1.6. Although LEPA had a plan to continue reliability operations in the event its control center became inoperable and had trained its operators on the plan, LEPA's contingency plan lacked procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan, as required by EOP-008-0 R1.5. LEPA's contingency plan also lacked procedures and responsibilities for providing annual training to ensure all LEPA operating personnel are able to implement the contingency plan, as required by EOP-008-0 R1.6.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although LEPA failed to demonstrate annual testing of its contingency plan, LEPA did provide operator sign-in sheets for training on the contingency plan, demonstrating that its operators were familiar with the components of the contingency plan. Furthermore, LEPA provided evidence that this operator training occurred annually and the contingency plan was reviewed and updated at least semi-annually to ensure viability of the plan.	On March 8, 2012, LEPA completed a series of modifications to the LEPA Energy Control Center Operating Procedures to address the requirements of EOP-008-0 R1.5 and R1.6. These modifications include procedures and designation of responsibilities for conducting periodic tests, at least annually, to ensure LEPA's Back-up Control Center Plan (Plan) is current. Additionally, LEPA added procedures and responsibilities for providing annual training to ensure that LEPA's operating personnel are able to implement the Plan. The Plan now includes procedures as follows: -The Back-Up Control Center will be tested at least annually. -Specific members of LEPA management and staff have responsibility for overseeing the testing of the Plan and the training of LEPA System Operators; -Testing and training will be done using real life situations; -LEPA System Operators shall demonstrate proficiency in all areas of LEPA's Plan; and -Additional documentation and records will be maintained to ensure compliance with EOP-008-0 R1.5 and R1.6.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Midwest Energy, Inc. (Midwest)	NCR01118	SPP201000366	TOP-002-1	R11	On July 30, 2010, Midwest, as a Load Serving Entity (LSE) and a Transmission Operator (TOP), self-certified noncompliance with TOP-002-1 R11 because it had been relying on seasonal, next-day, and current-day studies performed by the Southwest Power Pool Reliability Coordinator (SPP RC) to determine its System Operating Limits (SOLs), without performing an independent review of these studies. Consistent with Midwest's TOP-002-1 Normal Operations Planning procedure for current and next day planning, Midwest supplied its transmission and generation facility status to its host Balancing Authority (BA) on a real-time and day-ahead basis. The data was then forwarded to the SPP RC for inclusion in the SPP RC operation planning model. The procedure then stated that SPP RC "would perform a comprehensive analysis of system topology and transmission facility loading and determine if any corrective actions need[ed] to be implemented to conform with . . . reliability requirements." Such corrective actions might "include denial of requested outages for transmission or generation facilities . . . not considered secure and reliable under the proposed conditions." Regarding seasonal planning, Midwest was relying on SPP RC's "operational seasonal planning models developed in coordination with all impacted stakeholders . . . [and] based on the Model Development Working Group (MDWG) seasonal planning models for the current year." Finally, the Midwest procedures provided that Midwest would relay any deviations from scheduled system configurations to the SPP RC and neighboring systems immediately. SPP RE determined that Midwest's reliance on studies performed by the SPP RC, without further review by Midwest, does not comply with the requirements of TOP-002-1 R11. Further, SPP RE determined that an agreement between the SPP RC and Midwest stating that SPP RC would perform the studies for Midwest, must exist to ensure the continuing provision of the studies, as required by this Standard.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because compensating measures existed at the time the issue occurred. First, Midwest provided sample communications to demonstrate that it was coordinating its outages with both the SPP RC and surrounding TOPs. Second, Midwest indicated that following identification of any SOLs violations, SPP RC contacts it by telephone to discuss potential mitigation strategies and implement Transmission Loading Relief (TLR) procedures, as necessary. Midwest provided line outage requests submitted by its BA to SPP RC, which displayed outages in various stages of planning and/or implementation. The small size (392 MW peak load) of the Midwest system, combined with the evidence of outage coordination with surrounding TOPs and the SPP RC, reduced the risk created by Midwest's failure to conduct independent system studies or independent reviews of the studies conducted by the SPP RC.	Midwest executed a Study Agreement with the SPP RC which provides for the performance of next-day, current-day, and Real-Time Contingency Analysis (RTCA) results to be made available on an ongoing basis to Midwest's operating personnel. Midwest fully implemented the agreement into its TOP-002 Normal Operations Planning procedure on November 14, 2011. In addition Midwest has also formalized a process for seasonal studies to be performed and disseminated to operating personnel on a regular basis. SPP RE, during an on-site audit, verified completion of mitigation.
Southwest Power Pool Regional Entity (SPP RE)	Western Farmers Electric Cooperative (WFEC)	NRC01160	SPP201000443	TOP-002-1	R11	On October 28, 2010, as a Transmission Operator (TOP), WFEC self-reported an issue with TOP-002-1 R11. WFEC indicated that prior to September 13, 2010, it relied solely on next-day and current-day Bulk Electric System (BES) studies provided by the Southwest Power Pool, Inc., (SPP) for use in determining WFEC's System Operating Limits (SOLs). However, on September 13, 2010, SPP advised WFEC that it was not performing these studies on WFEC's behalf, but instead was performing the studies in support of its role as a Reliability Coordinator. At that time, no formal agreement existed between WFEC and SPP for the provision of the studies, and as a result, no mechanism ensured that WFEC would continue to receive the information necessary to perform accurate next-day and current-day BES analyses for determining SOLs, as required by TOP-002-1 R11. Prior to September 13, 2010, WFEC required its operators to perform the following activities during each 12 hour shift: (1) review any unacknowledged alarms on the Energy Management System (EMS); (2) review current-day and next-day load forecasts and make adjustments as necessary; and (3) check the SPP current-day and next-day contingency and voltage analysis and flow gates. Following the operators review of the designated items, the operator was required to sign and date a review completion check list. After September 13, 2010, WFEC continued to review posted SPP studies, and also began performing weekly studies of its own, while continuing to monitor its system daily for impending SOL violations. On March 28, 2011, WFEC entered into an agreement with SPP in which SPP agreed to ensure to continue providing next-day and current day studies to allow WFEC to identify its SOLs.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although no formal agreement initially existed between WFEC and SPP for the provision of the studies, WFEC's system operators were using, on a daily basis, the information provided by SPP to sufficiently identify SOLs prior to September 13, 2010. Also, the WFEC system was and still is continuously monitored by WFEC's EMS, which provides alarms of any impending SOL violations, thus reducing the risk to the BPS. Finally, WFEC's engineering staff performed in-house studies, which were similar to those provided by SPP, until WFEC entered into an agreement with SPP that ensured SPP would continue to provide current and next-day system studies.	In January 2011, WFEC entered into an agreement with the SPP to perform its next-day and current-day studies. The SPP performs these studies and uploads the documents to its website. Each morning, WFEC's TOPs are notified by SPP via email that the studies have been posted. After reviewing the study, the WFEC system operator makes a notation in the daily log book that the studies have been reviewed and take steps to address any identified SOL changes. The system operators place the studies electronically into WFEC's Compliance Program in accordance with WFEC Operating Procedure, "Performance, Review, and Documentation of Seasonal, Next-Day, and Current-Day Bulk Electric System Studies to Determine SOLs." The study results are made available to TOPs and Balancing Authorities (subject to confidentiality requirements) upon request.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Texas-New Mexico Power Co (TNMP)	NCR04143	TRE201100267	EOP-008-1	R1	During an Audit, dated February 11, 2011, Texas RE found that TNMP's interim provisions for the continuation of reliability operations within one hour of implementation of TNMP's contingency plan for loss of primary control facility were undocumented. The issue was May 4, 2010, the date TNMP was registered as a Transmission Operator (TOP) and became subject to this Standard, to July 15, 2010, the date Revision 3 to TNMP's Control Center Contingency Plan went into effect. Revision 3 adequately addressed the requirements of this Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The issue is documentation related. TNMP had implemented interim provisions for the continuation of reliability operations and had the necessary tools in place to continue the operations. However, the process remained undocumented for a period of two and a half months. Prior to completing its new Emergency Working Operations Center (EWOK) on August 1, 2009, TNMP had utilized its Mobile Operations Center to serve as a backup control facility in the event of an emergency at its primary Systems Operating Center. When the EWOK became operational, TNMP implemented a back-up slave console at its Gulf Coast Region Office (GCRO), located nearby the primary control facility. Thus, TNMP's operators could access the GCRO during the time it would take other TNMP operators to travel to the EWOK. TNMP has attested that TNMP would have followed this procedure, despite the fact that it was not formally documented during the period of this issue.	TNMP mitigated the issue associated with this standard by documenting its Emergency Operations Procedure. This was done on July 15, 2010. Texas RE verified all mitigation activities were complete.
Texas Reliability Entity, Inc. (Texas RE)	Luminant Energy Company, LLC	NCR10133	TRE201100393	VAR-002-1.1b	R3.2	On July 12, 2011, Luminant, as a Generator Operator, submitted a Self-Report for a failure to notify its Transmission Operator (TOP) within 30 minutes of a status or capability change on any other Reactive Power resources under its control and the expected duration of the change in status or capability, as required by this Standard. Namely, Luminant failed to notify the TOP within 30 minutes of an expected outage for a capacitor bank under its control. The capacitor bank outage occurred on May 22, 2011 at 09:33 Central Standard Time and notification of the estimated duration of the outage was not made until two days later on May 24, 2011 at 10:19 Central Prevailing Time. Luminant notified within 30 minutes the TOP of a reactive power resource issue, but did not inform the TOP of the expected duration of the outage. The reason given by Luminant for not communicating the duration was that the operator believed the issue was temporary due to a relay lockout, but in fact it was an equipment issue that was discovered and rectified on May 24, 2011. Regardless of the reason for the capacitor bank outage, Luminant should have timely communicated an estimated duration to the TOP on May 22, 2011.	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 an additional capacitor bank was in place to provide additional reactive capability, the plant operator had the capacity and capability of maintaining the voltage limits specified in the Voltage Profile published by the TOP at all times, and the issue was fairly brief, lasting approximately two days. Additionally, Luminant was aware that there was an outage issue with the capacitor bank and did notify the TOP of the outage, even though it failed to notify the TOP of the expected duration of the outage. When Luminant became aware that the outage was caused by equipment issues, Luminant communicated that information to the TOP on May 22, 2011 as well.	Luminant reported the estimated duration of the capacitor bank outage approximately two days after it was initially discovered. Additionally, Luminant installed capacitor bank alarming in the control room that annunciates whenever the capacitor bank status changes and informs the operator to notify the TOP of the nature and expected duration of the status change. Also, Luminant developed site specific procedures for capacitor bank operation and reporting and conducted NERC compliance training with staff regarding VAR-003. Finally, Luminant developed and distributed a "pocket manual" to its generation fleet describing reporting obligations associated with VAR-002-1.1b R3. Mitigation has been completed as of October 27, 2011.
Texas Reliability Entity, Inc. (Texas RE)	San Miguel Electric Cooperative, Inc. (SMEC)	NCR00253	TRE201100309	FAC-008-1	R1.1	On March 30, 2011, SMEC, as a Generator Owner, self-reported an issue with FAC-008-1 R1 because its Facility Ratings Methodology (FRM) did not include language stating that a Facility Rating shall equal the most limiting applicable equipment rating of the individual equipment that compromises that Facility. However, SMEC's reviewed rating did reflect the most limiting equipment rating. The duration period for this issue was from September 3, 2008, when the deficient FRM was adopted, until September 13, 2011, the date SMEC updated its FRM with the missing term "limited equipment."	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 SMEC's FRM did not include language stating that a Facility Rating shall equal the most limiting applicable equipment rating of the individual equipment, the actual rating determined and provided to the Electric Reliability Council of Texas, Inc. did reflect and consider the most limiting rating. The added language "limiting equipment" provided greater clarity to the reader that this term considers transmission conductors, terminal equipment, series and shunt compensation devices, ambient conditions, operating limitations and other assumptions.	SMEC updated the FRM on September 13, 2011 to include the previously missing term "limited equipment." All managerial and operational personnel that rely upon this information was apprised of the updates.

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)	San Miguel Electric Cooperative, Inc. (SMEC)	NCR00253	TRE201100310	FAC-009-1	R1	On March 30, 2011, SMEC, as a Generator Owner, self-reported an issue with FAC-009-1 R1 because SMEC did not establish Facility Ratings that are consistent with its Facility Ratings Methodology (FRM). The effective FCM at the time of this issue was discovered stated that "SMEC does not establish emergency ratings for the generator," which would mean that normal ratings equal emergency ratings. Yet SMEC's Resource Asset Registration Form (RARF) and Planning Model generator data included ratings that were higher than the normal ratings provided, suggesting an emergency rating did exist that was different than the normal ratings and was assigned different value. The narrative in the FRM did not match the ratings data in the RARF and Planning Model, so the SMEC modified the higher ratings to match the FRM narrative. To remedy this issue, SMEC chose to modify the actual emergency ratings of its generator to equal its normal rating which is equivalent to not having a different emergency rating. The duration period for this issue was from September 3, 2008 until January 31, 2012, the date SMEC modified its emergency ratings. The purpose of that "Emergency" rating was to set a higher rating at times when the SMEC's adjacent lignite mine was shut down. The generator gross MW would stay the same. The mine load was being included as an auxiliary load for the generating plant.	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 the original emergency rating provided to the Electric Reliability Council of Texas, Inc. in the RARF was a rating that reflects SMEC's facility capabilities. The purpose of that emergency rating was to set a higher rating at times when the SMEC's adjacent lignite mine was shut down and the mine's load was being included as an auxiliary load for the generating plant. However, the generator gross MW capacity remained the same and the rating reflected SMEC's facility actual capabilities.	SMEC modified the emergency ratings of its generator to equal its normal rating on January 31, 2012. SMEC also updated its FRM on September 13, 20122 to reflect this revision and all personnel that rely upon this information were apprised.
Western Electric Coordinating Council (WECC)	California Department of Water Resources (CDWR)	NCR05047	WECC2012009802	CIP-001-1	R3	Between February 14, 2012, and February 24, 2012, WECC conducted an audit of CDWR. While during the course of the audit, the Audit Team determined that CDWR documented procedures for the recognition of, and for making operating personnel aware of, sabotage events on its facilities pursuant to CIP-001-1 R1. The Audit Team also determined that CDWR, as a Generator Operator and Load Serving Entity, could not provide evidence that it provided CDWR operating personnel with these procedures, including personnel to contact for reporting sabotage events, between June 18, 2007, and January 31, 2009. CDWR provided the Audit Team with emails evidencing that CDWR provided operating personnel with sabotage event procedures and contacts lists to be used for reporting sabotage events after January 31, 2009. Prior to that date, however, CDWR could not provide evidence demonstrating that operating personnel received this information.	This issue posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system. The Audit Team determined that operating personnel were familiar with sabotage procedures as a matter of standard operating practice within CDWR. Operating personnel were familiar with how to recognize a sabotage event. Further, although documentation was not provided, operating personnel were generally aware of the appropriate party to contact within CDWR given a sabotage event.	During the course of the audit, CDWR provided evidence that demonstrated it provided operating personnel with sabotage response guidelines as of January 31, 2009.
Western Electric Coordinating Council (WECC)	NorthWestern Corporation (NWC)	NCR05282	WECC2012009125	TOP-007-WECC-1	R2	On January 10, 2012, NWC, as a Balancing Authority, Transmission Operator, Transmission Owner, Generator Owner, Load Serving Entity and Transmission Planner, submitted a Self-Report stating that in its capacity as the Path Operator for WECC Path18, NWC discovered that Path 18 was overscheduled by five (5) MW on November 22, 2011, hour ending 1900. WECC reviewed NWC's Self-Report and determined that the root cause of the issue stemmed from an error in a User Defined Interface (AMPS) used to monitor the activity on Path 18. A change was made in error to the AMPS Interface that temporarily removed the real time hour ahead wind schedules from the AMPSS total. This allowed real time schedules to be implemented resulting in a 5 MW over schedule of Path 18 for the Hour Ending (HE) 1900.	This issue posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system. The System Operating Limit (SOL) on Path 18 for the hour ending in 1900 was 337 MW. NWC overscheduled the path by 5 MW, less than 2% of the SOL. Further, actual flows did not exceed the Operating Transfer Capability Limits associated with HE 1900. The overscheduled duration lasted for a period of an hour and was immediately corrected.	NWC completed the following mitigation activities: 1) NWC implemented new templates and interfaces in AMPS to be used by the Day Ahead and System Operator responsible for Hour Ahead Scheduling; and 2) the NWC Transmission Services Department held internal training with pre-schedulers to discuss implications of exceeding SOLs and measures that were implemented in AMPS to prevent this type of error in the future.
Western Electricity Coordinating Council (WECC)	Colorado Springs Utilities (CSU)	NCR05106	WECC2012009506	FAC-009-1	R1	On January 24, 2012, CSU, as a Transmission Owner and Generator Owner, self-certified potential noncompliance with FAC-009-1 R1.2. On January 30, 2012, a WECC Subject Matter Expert (WECC SME) contacted CSU to discuss its self-certification. According to the WECC SME, CSU stated that on November 30, 2011, it discovered that its backup over current relays and current transformers (CTs) located on its Bulk Electric System (BES) transformers were not included in its analysis of its facility ratings, in accordance with its Facility Ratings Methodology. CSU has five 230-115 kV transformers – two at its Cottonwood Substation, two at its Kelker Substation, and one at the Nixon Substation. On November 30, 2011, CSU was in the process of updating its BES transformer rating spreadsheet and discovered that backup over current relays and CTs current transformers on its transformers at the substations described above were not included in the results of its facility ratings conducted on June 18, 2007.	These CT and PT devices are the most limiting factor. The Transmission Operators were notified of the de-ratings the same day as the discovery of the problems. For these reasons, WECC determined this issue posed minimal risk to the reliability of the bulk power system.	CSU completed the following mitigation activities: 1. The Transmission Operators were notified of the de-ratings the same day as the discovery of the problems. The Transmission Operators were notified of Nixon #1 transformer de-rating via telephone call and then a follow-up e-mail. The Transmission Operators were notified of the Cottonwood #5 transformer de-rating via e-mail; 2. A review of all CT ratings and protective relay setting for the BES transformers was completed; 3. A new BES transformer spreadsheet was be finished that lists each piece of terminal equipment (including relays and CTs) separately so the limit can be readily identified; 4. The CSU process document with roles and responsibilities was reviewed, updated, and distributed internally for FAC-009-1. All supervisors with FAC- 009 responsibilities were reminded of the importance of following the Ratings Methodology; and 5. CSU changed the CT ratio and relay settings so that the original ratings of the BES transformers that were de-rated could be restored.

Attachment A-2

May 30, 2012 Public CIP - Find Fix and Track 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) Hardee Power Partners Limited (HPS)	NCRXXXXX	FRCC2012009741	CIP-002-3	R4	FRCC_URE1 self-certified an issue with CIP-002-3 R4 using the Self-Certification form. FRCC_URE1 did not timely complete the annual Critical Asset (CA) and Critical Cyber Asset (CCA) list and risk-based assessment methodology (RBAM), with approval signed and dated by the senior manager. FRCC_URE1 did timely complete a RBAM application review as part of its response to the NERC survey and timely identified all its CAs and CCAs but did not document the signatures of the senior manager. FRCC_URE1 stated that the list has not changed in the prior two years. The signed RBAM approval and list of CAs and CCAs was completed 26 days past the required date.	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 did timely complete a RBAM application review as part of its response to the NERC survey and timely identified all its CAs and CCAs but did not document the signatures of the senior manager. FRCC_URE1 was only 26 days late in documenting the annual review, and the annual review and assessment identified no CCAs and no additional CAs.	FRCC_URE1 completed mitigation activities by obtaining the senior manager's signed and dated approval. Second, FRCC_URE1 scheduled its review(s) for the next two years. FRCC_URE1 also discussed the issue with the personnel responsible for RBAM application and emphasized timely completion of all required compliance activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC2012010064	CIP-004-3	R2; R2.3	FRCC_URE2 self-reported an issue with CIP-004-3 R2.3 because one of its contractors did not complete his required annual cyber security training when his annual training expired. He had authorized logical access to Critical Cyber Assets and it was discovered 64 days later, when he accessed the systems after a long gap, that his training was expired. Upon discovery of the expired annual training, the contractor's access was revoked. The subject contractor completed a successful training the following day. Thus, the duration of the issue was 65 days. The concerned contractor was previously trained in prior years. FRCC_URE2 originally self-reported an issue with CIP-007-3 R5, but following FRCC review and guidance, FRCC_URE2 corrected and re-submitted the Self-Report for the correct CIP Standard and requirement, as described in the previous paragraph.	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 the subject contractor had previously completed training , and the last course had no significant updates. Further, the contractor was a trusted vendor with a valid long-term contract and a valid personnel risk assessment. The contractor promptly completed the training refresher with the resultant delay of two months. During that time, he had access to Cyber Assets only once. Although FRCC_URE2 has violated this Standard previously, the instant issue nonetheless does not represent recurring conduct. The prior violation involved an employee who only received partial training, whereas this issue relates to contractor training. Further, the previous instance was recorded in the early stages of CIP-004-2 R2 compliance for initial training. Following the prior violation, FRCC_URE2 updated many controls and imparted training to all responsible for controlling access. In the current instance, the training lapse resulted from the extended absence of the contractor.	FRCC_URE2 completed mitigation activities by having the contractor complete the required annual training. Additionally, FRCC_URE2 conducted activities including one-on-one discussion and additional awareness training for FRCC_URE2 personnel involved with handling of contractor engagements, in order to improve awareness of mandatory annual retraining requirements for those involved with the process.
Midwest Reliability Organization (MRO) and Reliability*First* Corporation (ReliabilityFirst)	Unidentified Registered Entity 1 (URE1)	NCRXXXXX	MRO201100436; RFC2011001252	CIP-007-3	R3; R3.1	URE1 self-reported noncompliance with Reliability Standard CIP-007-3 R3 because it failed to assess applicability of a security patch for a certain software within 30 days. The application security patch was assessed and installed 11 days after the 30-day time window required by CIP-007-3 R3.1. The entity's Energy Management System (EMS) group utilizes two methods for identifying updates and security patches for applications installed on EMS Cyber Assets residing within the Electronic Security Perimeter (ESP). Most scheduled and out-of-cycle updates for another application are downloaded automatically consistent with the monthly patch release process. Patches and upgrades for other applications, such as the application at issue, are obtained from a number of software vendors, each with their own notification system and patch or upgrade release schedule. The downloading and assessment of patches to these applications is a manual process previously assigned to one of the EMS system administrators. The EMS system administrator to whom responsibility was assigned for monitoring and assessing application security patches and upgrades resigned from URE1. When transitioning his responsibilities to the other two EMS system administrators, the individual failed to transfer the contact information for the application patch release notification to his fellow system administrators. As a result, the security patch notification did not reach the two EMS system administrators. One of the EMS system administrators observed that he had not seen any change control tickets to update the application. He proceeded to log into the application's website to check for the most recent security patch releases. He found that a security update had been released 41 days prior. The system administrator was able to assess and install the security patch on the same day; however, he recognized the patch was assessed 11 days after the 30-day window required by CIP-007 R3.1 and reported the issue to his supervisor.	The issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because URE1 only missed one patch for a short period of time, and that patch dealt with document-reader software installed on machines without internet access. Additionally, the software was only enabled in the "Protected Mode," which prevents and restricts security vulnerabilities.	Upon discovering the missing security patch, the system administrator immediately proceeded to download, assess, test and install the security patch on the application. The system administrator then checked and confirmed that all applications installed on EMS Cyber Assets residing within the ESP were running the latest security patch releases. To mitigate the issue and preclude recurrence, URE1 revised its security patch management monitoring and assessment process for applications that are not downloaded automatically and are residing within the ESP as follows: (1) confirmed that correct EMS contact information was contained in all associated vendor patch release notification systems; (2) revised the EMS security patch management procedure for applications to require personnel to check with each vendor for security patch releases every 30 calendar days; and (3) added a list of the applications and their respective vendors to the procedure.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE1) Moorhead Public Service (MPS)	NCRXXXXX	MRO2012009154	CIP-003-1	R2	MRO_URE1 self-certified noncompliance with CIP-003-1 R2 because it failed to assign a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-1 through CIP-009-1.	The issue posed a minimal risk and did not pose serious or substantial risk to the reliability of the bulk power system because although the entity failed to have a policy appointing a senior manager in charge of the responsibilities for CIP-002-3 through CIP-009-3, MRO_URE1 did have an unassigned senior manager in charge. This senior manager was ultimately assigned as the senior manager per the Standard.	MRO_URE1's general manger authorized and approved a policy that designates the electrical engineering manager as the single senior manager with overall responsibility and authority for leading and managing the entity's adherence to CIP-002-3 through CIP-009-3. MRO verified that the entity completed its Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE2)	NCRXXXXX	MRO201100437	CIP-004-1	R4; R4.1	During a spot check, MRO determined that MRO_URE2 failed to perform quarterly reviews of physical and cyber access for a six-quarter period. The access rights of users were not reviewed quarterly for a installed system, which is used in performing backups of Critical Cyber Assets, as well as workstations at the backup control center. The backup system is only accessed by five individuals, all of whom were involved in the installation of the system and have proper access. The workstations have only two accounts on them - one for use by system operators in the event that MRO_URE2 would need to relocate to its backup center, and a single administrative account. This account is only accessible by one individual, a long-term employee that is the primary administrator for all CIP workstations and whose access was reviewed quarterly for CIP workstations that did not reside at the backup control center.	The issue posed a minimal risk and did not pose serious or substantial risk to the reliability of the bulk power system because the backup system is only accessed by five individuals, all of whom were involved in the installation of the system and have proper access. The workstations have only two accounts on them - one for use by system operators in the event that the entity would need to relocate to its backup center, and a single administrative account. This account is only accessible by one individual, a long-term employee that is the primary administrator for all CIP workstations and whose access was reviewed quarterly for CIP workstations that did not reside at the backup control center. Furthermore, these workstations reside on a separate network from the primary Energy Management System and are powered off except for periodic checks and patch installation. For both of the workstations and the backup system, accounts were reviewed annually as part of MRO_URE2's annual vulnerability assessment. Additionally, MRO_URE2 has not needed to operate its backup control center or use the workstations related to this issue, other than for the purpose of maintaining them, and MRO_URE2 did not have any reportable cyber incidents during the period.	MRO_URE2 performed the following actions to mitigate the issue: (1) identified missing devices and associated accounts on the quarterly access review reports; (2) updated the quarterly access review reports to include omitted information; and (3) conducted the quarterly access review and verified that objectives were met. MRO verified that MRO_URE2 completed its Mitigation Plan.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE2)	NCRXXXXX	MRO201100438	CIP-005-1	R2; R2.5.3	During a spot check, MRO determined that MRO_URE2 failed to perform quarterly reviews of the access rights of users for access point devices in accordance with CIP-005-1 R2.5.3. Specifically, MRO_URE2 was unable to provide evidence that it performed reviews of access point devices for a six-quarter period. The access point devices are only accessed by two employees.	The issue posed a minimal risk and did not pose serious or substantial risk to the reliability of the bulk power system because the access point devices are only accessed by two employees, and both employees are responsible for other CIP assets which did have quarterly access reviews performed. MRO_URE2 also has an intrusion detection system to alert it of unauthorized access to the Electronic Security Perimeter, and the accounts on all access point devices were reviewed annually as part of the entity's annual vulnerability assessment. Additionally, MRO_URE2 did not have any reportable cyber incidents during the period.	MRO_URE2 performed the following actions to mitigate the issue: (1) identified missing devices and associated accounts on the quarterly access review reports; (2) updated the quarterly access review reports to include omitted information; and (3) conducted the quarterly access review and verified that objectives were met MRO verified that the entity completed its Mitigation Plan.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1) FirstEnergy Generation Corp. (FE Genco)	NCRXXXXX	RFC2011001046	CIP-006-1	R1; R1.1	RFC_URE1 self-reported an issue with CIP-006-1 R1 to Reliability*First.* RFC_URE1 did not enclose within conduit two sections of cable located outside a Physical Security Perimeter (PSP). The first section of unenclosed cable is approximately 36 feet long, and the second section of unenclosed cable is approximately 159 feet long. Both sections of cable are located in the same RFC_URE1 generating facility.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The two sections of cable are located in the same RFC_URE1 generating facility which is protected by physical security measures including perimeter fencing, surveillance cameras, and security guards who remain on duty twenty-four hours a day, seven days a week. Further, access to the generating facility in which the cables reside is restricted to only those individuals with approved key card access. Additionally, the cables reside above a suspended ceiling thereby reducing access due to the height of the ceiling. Finally, the cables reside with a number of non-critical cables of the exact same type and color, thereby making identification of the cables difficult.	RFC_URE1 placed the 36 foot section of the cable at issue, as well as the 159 foot section of the other cable at issue, in conduit, thereby creating a complete “six-wall” border pursuant to CIP-006-1 R1.1.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012009862	CIP-002-1	R1; R1.1	Reliability*First* conducted a compliance audit to assess RFC_URE2’s compliance with applicable CIP Reliability Standards (Compliance Audit). During this Compliance Audit, Reliability*First* discovered that two versions of RFC_URE2’s risk-based assessment methodology (RBAM) were not in fact risk-based. These methodologies simply stated the types of facilities that RFC_URE2 would review annually. These methodologies also concluded that RFC_URE2 characteristics rendered it unable to “impact the Bulk Electric System.” RFC_URE2 stated that it would evaluate its ability to impact the bulk power system (BPS) annually. Reliability*First* determined that RFC_URE2 had an issue with the Standard as these versions of RFC_URE2’s RBAM did not document RFC_URE2's procedures and evaluation criteria.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. While the RBAM was incomplete, it provided some indication of what types of assets to include, which was corroborated by the later finding of no assets. Although RFC_URE2’s RBAM was found to be deficient, Reliability*First* found that RFC_URE2’s determination that it had no Critical Assets, and therefore no Critical Cyber Assets, was correct. This determination was confirmed when RFC_URE2 implemented its updated RBAM. In addition, the RBAM took into consideration RFC_URE2’s interconnection points and load size.	RFC_URE2 submitted to Reliability*First* a Mitigation Plan to address the issue with of CIP-002-1 R1. In this Mitigation Plan, RFC_URE2 memorialized that it updated and implemented its revised RBAM. Reliability*First* verified this completion via evidence reviewed at RFC_URE2’s compliance audit.

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	RFC2012009863	CIP-002-3	R2	Reliability*First* conducted a compliance audit to assess RFC_URE2's compliance with applicable CIP Reliability Standards (Compliance Audit). During Reliability*First* 's Compliance Audit of RFC_URE2, RFC_URE2 failed to provide evidence of its annual application of its risk-based assessment methodology (RBAM). Accordingly, RFC_URE2 failed to show that it developed a list of Critical Assets, as required by CIP-002-3 R2, and associated Critical Cyber Assets, as required by CIP-002-3 R3. RFC_URE2 also failed to show that its senior manager had approved its RBAM, its list of Critical Assets, and its list of Critical Cyber Assets, as required by CIP-002-3 R4. As a result, Reliability*First* identified an issue with CIP-002-3 R2.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Throughout the time period of this issue, RFC_URE2 self-certified to Reliability*First* that it was in conformity with CIP-002-3 R2, R3 and R4. RFC_URE2's self-certifications were based on its own review of its RBAM and its lists of Critical Assets and associated Critical Cyber Assets. While the RBAM was incomplete, it provided some indication of what types of assets to include, which was corroborated by the later finding of no assets. Although RFC_URE2's RBAM was found to be deficient, Reliability*First* determined that RFC_URE2's determination that it had no Critical Assets, and therefore no Critical Cyber Assets was correct. In addition, the RBAM took into consideration RFC_URE2's interconnection points and load size.	RFC_URE2 submitted to Reliability*First* a Mitigation Plan to address issue with CIP-002-3 R2. RFC_URE2's Mitigation Plan addressing its issue with CIP-002-1 R1 memorialized that it updated and implemented its revised RBAM. These actions also mitigated the issue with CIP-002-3 R2. RFC_URE2's Mitigation Plan addressing its issues with CIP-002-3 R2, R3 and R4 memorialized actions it took to revise its document retention policies to ensure that it retains evidence of the requisite annual reviews in the future.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012009864	CIP-002-3	R3	Reliability*First* conducted a compliance audit to assess RFC_URE2's compliance with applicable CIP Reliability Standards (Compliance Audit). During Reliability*First* 's Compliance Audit of RFC_URE2, RFC_URE2 failed to provide evidence of its annual application of its risk-based assessment methodology (RBAM). Accordingly, RFC_URE2 failed to show that it developed a list of Critical Assets, as required by CIP-002-3 R2, and associated Critical Cyber Assets, as required by CIP-002-3 R3. RFC_URE2 also failed to show that its senior manager had approved its RBAM, its list of Critical Assets, and its list of Critical Cyber Assets, as required by CIP-002-3 R4. As a result, Reliability*First* identified an issue with CIP-002-3 R3.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Throughout the time period of this issue, RFC_URE2 self-certified to Reliability*First* that it was in conformity with CIP-002-3 R2, R3 and R4. RFC_URE2's self-certifications were based on its own review of its RBAM and its lists of Critical Assets and associated Critical Cyber Assets. While the RBAM was incomplete, it provided some indication of what types of assets to include, which was corroborated by the later finding of no assets. Although RFC_URE2's RBAM was found to be deficient, Reliability*First* determined that RFC_URE2's determination that it had no Critical Assets, and therefore no Critical Cyber Assets was correct. In addition, the RBAM took into consideration RFC_URE2's interconnection points and load size.	RFC_URE2 submitted to Reliability*First* a Mitigation Plan to address issue with CIP-002-3 R3. RFC_URE2's Mitigation Plan addressing its issue with CIP-002-1 R1 memorialized that it updated and implemented its revised RBAM. These actions also mitigated the issue with CIP-002-3 R3. RFC_URE2's Mitigation Plan addressing its issues with CIP-002-3 R2, R3 and R4 memorialized actions it took to revise its document retention policies to ensure that it retains evidence of the requisite annual reviews in the future.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012009865	CIP-002-3	R4	Reliability*First* conducted a compliance audit to assess RFC_URE2's compliance with applicable CIP Reliability Standards (Compliance Audit). During Reliability*First* 's Compliance Audit of RFC_URE2, RFC_URE2 failed to provide evidence of its annual application of its risk-based assessment methodology (RBAM). Accordingly, RFC_URE2 failed to show that it developed a list of Critical Assets, as required by CIP-002-3 R2, and associated Critical Cyber Assets, as required by CIP-002-3 R3. RFC_URE2 also failed to show that its senior manager had approved its RBAM, its list of Critical Assets, and its list of Critical Cyber Assets, as required by CIP-002-3 R4. As a result, Reliability*First* identified an issue with CIP-002-3 R4.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Throughout the time period of this issue, RFC_URE2 self-certified to Reliability*First* that it was in conformity with CIP-002-3 R2, R3 and R4. RFC_URE2's self-certifications were based on its own review of its RBAM and its lists of Critical Assets and associated Critical Cyber Assets. While the RBAM was incomplete, it provided some indication of what types of assets to include, which was corroborated by the later finding of no assets. Although RFC_URE2's RBAM was found to be deficient, Reliability*First* determined that RFC_URE2's determination that it had no Critical Assets, and therefore no Critical Cyber Assets was correct. In addition, the RBAM took into consideration RFC_URE2's interconnection points and load size.	RFC_URE2 submitted to Reliability*First* a Mitigation Plan to address issue with CIP-002-3 R4. RFC_URE2's Mitigation Plan addressing its issue with CIP-002-1 R1 memorialized that it updated and implemented its revised RBAM. These actions also mitigated the issue with CIP-002-3 R4. RFC_URE2's Mitigation Plan addressing its issues with CIP-002-3 R2, R3 and R4 memorialized actions it took to revise its document retention policies to ensure that it retains evidence of the requisite annual reviews in the future.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3) LSP University Park, LLC (LSP University Park)	NCRXXXXX	RFC2012009869	CIP-002-3	R1	Reliability*First* conducted a compliance audit of RFC_URE3 (Compliance Audit). During the Compliance Audit, Reliability*First* discovered an issue with CIP-002-3 R1. RFC_URE3 failed to maintain a risk-based assessment methodology (RBAM) as required by CIP-002-3 R1. RFC_URE3's RBAM consisted of one question: "Does an asset, if destroyed, degraded, compromised or otherwise rendered unavailable, adversely impact the reliability or operability of the Bulk Electrical System (BES)?" The RBAM defined three possible impact determinations: "Low," "Medium," and "High," providing only minimal descriptions of the criteria for each category. The RBAM provided no additional guidance on how to choose a category for a particular asset, or how to determine whether the loss of the plant will fall into one of the categories. Since the RBAM did not provide sufficient guidance to a user, it was not effectively risk-based.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. While the RBAM was incomplete, it provided some indication of what types of assets to include, which was corroborated by the later finding of no assets. In addition, RFC_URE3 has no Critical Assets and therefore inherently presents minimal risk to the BPS. Despite the described shortcomings of RFC_URE3's RBAM, Reliability*First* 's audit team determined that RFC_URE3 had properly declared no Critical Assets.	RFC_URE3's operational responsibilities shifted from one company to another company. After the Compliance Audit, RFC_URE3 implemented a new RBAM based on the new company's standard methodology. RFC_URE3 provided the new RBAM to Reliability*First* and Reliability*First* verified that RFC_URE3 mitigated the issue as of that date.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity (SERC_URE1) Birchwood Power Partners, L.P. (Birchwood)	NCRXXXXX	SERC2011008611	CIP-002-1	R4	The SERC CIP audit team reported an issue with CIP-002 R4, stating that SERC_URE1, failed to provide evidence showing that the senior manager or delegate(s) annually approved the risk-based assessment methodology (RBAM), the list of Critical Assets, and the list of Critical Cyber Assets (CCAs). SERC staff determined that SERC_URE1 had failed to assign in writing a senior manager with responsibility for SERC_URE1's implementation of, and adherence to, the CIP standards until that responsibility was assigned in writing to a SERC_URE1 business manager. As a result, despite the fact that a SERC_URE1 manager had signed and approved RBAMs with null lists for Critical Assets and CCAs in two instances, the manager was not a valid signer because he or she had not been assigned responsibility in writing for SERC_URE1's compliance with the CIP standards. SERC_URE1 also had an RBAM with null lists for Critical Assets and CCAs but could not provide evidence that it had been signed. Therefore, the issue extends back to Version 1 of the Standard.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4; and 2. Although a SERC_URE1 manager had not been properly delegated responsibility for SERC_URE1's compliance with the CIP standards, the manager reviewed and approved SERC_URE1's RBAMs with null lists for Critical Assets and CCAs in two instances indicating that SERC_URE1 did not acquire any Critical Assets or CCAs in 2010.	SERC staff verified that SERC_URE1 completed the following actions: SERC_URE1 revised its Internal Compliance Program (ICP) to clarify details of the annual Critical Asset Identification self-assessment. The ICP now requires the senior manager or delegate to sign the self-assessments and file at the facility.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity (SERC_URE1) Birchwood Power Partners, L.P. (Birchwood)	NCRXXXXX	SERC2011008612	CIP-003-1	R2	The SERC CIP audit team reported an issue with CIP-003-1 R2, stating that SERC_URE1 failed to provide evidence documenting the senior manager's delegation of authority to a named delegate in the same manner as R2.1 and R2.2, and failed to provide evidence of the senior manager's approval of the delegation of authority. SERC staff determined that SERC_URE1 was unable to provide evidence that it had assigned a senior manager with overall responsibility for leading and managing SERC_URE1's implementation of, and adherence to, Standards CIP-002 through CIP-009. Three months after the audit, a SERC_URE1's manager was assigned authority in writing to manage all aspects of the facility's NERC compliance program, including the CIP standards.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4; and 2. Although a SERC_URE1's manager had not been assigned responsibility in writing for SERC_URE1's compliance with the CIP standards, the manager was acting in that capacity.	SERC staff verified that SERC_URE1 completed the following actions: 1. SERC_URE1 assigned its manager authority in writing to manage all aspects of the facility's NERC compliance program, including the CIP standards; and 2. SERC_URE1 revised its Internal Compliance Program (ICP) to clarify details surrounding the CEO delegation, the senior manager delegation, delegations made by the senior manager and the requirement to document changes to the senior manager position within 30 days. The ICP now includes the designation of a single senior manager with overall responsibility and authority for leading and managing SERC_URE1's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity (SERC_URE2) French Broad Electric Membership Corporation (French Broad EMC)	NCRXXXXX	SERC2012009649	CIP-003-1	R2	SERC_URE2 self-certified an issue with CIP-003-1 R2, stating that it did not have documentation of the assignment of a single senior manager with overall responsibility and authority for leading and managing SERC_URE2's implementation of, and adherence to, Standards CIP-002 through CIP-009. SERC staff reviewed documentation showing that SERC_URE2 assigned its general manager with overall responsibility and authority for leading and managing SERC_URE2's implementation of, and adherence to, Standards CIP-002 through CIP-009 and identified the general manager by name, title, and the date of designation. The same documentation showed a proper delegation of authority from the general manager to a different manager on the same day.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4; and 2. SERC_URE2 is a minimal size utility.	SERC staff verified that SERC_URE2 completed the following action: SERC_URE2 established a corporate procedure, effective that met the requirements of CIP-003 R2 and identified the single senior manager with overall responsibility and authority for leading and managing implementation of, and adherence to, NERC Reliability Standards CIP-002 through CIP-009.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1) Kansas City Power & Light Company (KCPL)	NCRXXXXX	SPP201100554	CIP-002-3	R4	SPP RE_URE1 self-reported an issue with CIP-002-3 R4 related to approval of its Critical Asset list and its Critical Cyber Asset (CCA) list by the senior manager or his or her delegate(s). As required by CIP-002-3 R3, SPP RE_URE1 had developed a list of CCAs essential to the operation of its Critical Assets. However, SPP RE_URE1's senior manager did not approve the list of CCAs. Instead, the list approved by the senior manager was a high level consolidated list describing the CCAs, rather than a detailed component level inventory.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the CCAs list approved by the SPP RE_URE1's senior manager was not a detailed list of the CCA inventory, SPP RE_URE1 had developed a detailed list of CCAs. However, instead of approving the detailed list, the senior manager was approving a representative, high-level list of the CCAs. Further, the senior manager had approved SPP RE_URE1's Critical Asset list.	SPP RE_URE1 added the detailed list of CCAs to the annual approval document and has had the document approved by the senior manager or delegate.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2) Kansas City Power & Light- KCPL - Greater Missouri Operations (KCPLGMO)	NCRXXXXX	SPP201100565	CIP-002-3	R4	SPP RE_URE2 self-reported an issue with CIP-002-3 R4 related to approval of its Critical Asset list and its Critical Cyber Asset (CCA) list by the senior manager or his or her delegate(s). As required by CIP-002-3 R3, SPP RE_URE2 had developed a list of CCAs essential to the operation of its Critical Assets. However, SPP RE_URE2's senior manager did not approve the list of CCAs. Instead, the list approved by the senior manager was a high level consolidated list describing the CCAs, rather than a detailed component level inventory.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although the CCAs list approved by the SPP RE_URE2's senior manager was not a detailed list of the CCA inventory, SPP RE_URE2 had developed such a detailed list of CCAs. However, instead of approving the detailed list, the senior manager was approving a representative, high-level list of the CCAs. Furthermore, the senior manager had approved SPP RE_URE2's Critical Asset list.	SPP RE_URE2 added the list of CCAs to the annual approval document and has had the document approved by the senior manager or delegate.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201100263	CIP-005-1	R1	During an Audit, Texas RE found that Texas RE_URE1 failed to identify and document all access points to its Electronic Security Perimeter (ESP). Texas RE_URE1 had two system switches installed. The system switches unidirectionally transmit data outside the ESP via ports to the quality assurance system testing environment. Texas RE determined that Texas RE_URE1 has implemented technical controls to prevent incoming traffic; however, these ports, which transmitted outgoing traffic, were still considered access points and should have been identified as such. The start date of this issue is when Texas RE_URE1 failed to identify these access points to the ESP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the ports at issue were still being afforded the same protective measures of all other access points on the system, including firewalls, intrusion protection systems, and antivirus software. These ports were not identified as access points due to Texas RE_URE1's incorrect understanding of the definition of the term.	Since the Audit, Texas RE_URE1 has reconfigured it's network, eliminating the ports at issue and only allowing traffic to pass in/out of its ESP via firewalls. These ports were eliminated and documented. Texas RE_URE1's current network diagrams confirm that all access points have been documented. Texas RE verified all mitigation activities were complete.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201100266	CIP-007-1	R5; R5.2.1; R5.3.2; R5.3.3	During an Audit, Texas RE found that Texas RE_URE1 was noncompliant with R5.2.1, R5.3.2 and R5.3.3. First, Texas RE_URE1 did not disable shared administrator accounts on eight Cyber Assets, as required by R5.2.1. Texas RE_URE1 had implemented procedural controls to minimize and manage the scope of the enabled shared accounts. The assets associated with this issue were commissioned prior to the beginning of the noncompliance period. The noncompliance period was for eight months, from the day Texas RE_URE1 was required to comply with CIP-007 R5 for these assets, until the day Texas RE_URE1 disabled the shared accounts. Second, all of Texas RE_URE1's Cyber Assets authenticated by active directory are not capable of implementing technical controls that enforce strict compliance with the password requirements listed in R5.3.2. At the time of the audit, Texas RE_URE1 had not filed a Technical Feasibility Exception (TFE) request regarding these Cyber Assets. The duration of this issue was for two years, until Texas RE accepted Texas RE_URE1's TFE. Third, all Cyber Assets deployed within Texas RE_URE1's ESPs are not capable of implementing technical controls to enforce password expiration, as required by R5.3.3. At the time of the audit, Texas RE_URE1 had not filed a TFE for these Cyber Assets. The duration of this issue was for two years, until Texas RE accepted Texas RE_URE1's TFE.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Texas RE_URE1 had implemented procedural controls to minimize and manage the scope of the enabled shared accounts and passwords. Regarding subrequirement R5.2.1, Texas RE_URE1's procedure requires that users utilizing shared accounts manually record the tasks they perform and the date they were performed and that these logs be submitted to a Supervisory Control and Data Acquisition (SCADA) administrator. Regarding subrequirements R5.3.2.and R5.3.3, the risk was mitigated by the fact that during the noncompliance period, Texas RE_URE1 had administered training to its staff in order to ensure that passwords are created with the complexity required by R5.3.2 and are retired in accordance with R5.3.3.	Texas RE_URE1 had mitigated the issue associated with R5.2.1 by disabling shared accounts. Further, Texas RE_URE1 submitted TFEs addressing the issues associated with R5.3.2 and R5.3.3. These TFEs were accepted by Texas RE. Additionally, Texas RE_URE1 has implemented procedural controls in the form of a staff training to ensure that passwords are created with the complexity required by R5.3.2 and are retired in accordance with R5.3.3. Texas RE verified all mitigation activities were complete.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) Barney M Davis Unit 1 (Barney Davis)	NCRXXXXX	TRE201100511	CIP-003-3	R2.2	Texas RE_URE2 self-reported that its appointed single senior manager with overall responsibility and authority for leading and managing the Texas RE_URE2 implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3, left the company. Texas RE_URE2 CIP procedure identifying this senior manager, was not updated within 30 days of his departure, which presented an issue with CIP-003-3 R2.2. TRE determined that the issue duration was approximately four months, 30 days after the manager left, until Texas RE_URE2's internal compliance procedure was updated.	This issue did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS). Texas RE determined that based on the administrative nature of this issue, the availability of responsible leadership throughout the period, and Texas RE_URE2 's lack of Critical Assets, the risk to the reliability of the BPS was minimal. First, the senior manager that left reported to the replacement senior manager. When the appointed senior manager left, the replacement senior manager had already been on staff and at no point during the duration of this issue was Texas RE_URE2's NERC internal compliance program (ICP) left without leadership. In addition, Texas RE_URE2 is a small entity and all of its employees involved in NERC compliance knew at all times who was responsible for Texas RE_URE2's NERC ICP. Also, Texas RE_URE2 submitted an attestation that it did not have any Critical Assets during the time period of this issue.	Texas RE_URE2's internal cyber security procedure was updated to include the new single senior manager. The manager at the facility location and the compliance employees are aware of the updated document and its location, and have access to the document.

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 3 (Texas RE_URE3) Barney M Davis LP (Barney)	NCRXXXXX	TRE201100512	CIP-003-3	R2.2	Texas RE_URE3 self-reported that its appointed single senior manager with overall responsibility and authority for leading and managing the Texas RE_URE3's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3, left the company. Texas RE_URE3's CIP procedure identifying this senior manager was not updated within 30 days of his departure, which presented an issue with CIP-003-3 R2.2. TRE determined that the issue duration was approximately four months, 30 days after the manager left, until Texas RE_URE3's internal compliance procedure was updated.	This issue did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS). TRE determined that based on the administrative nature of this issue, the availability of responsible leadership throughout the period, and Texas RE_URE3's lack of Critical Assets, the risk to the reliability of the BPS was minimal. First, the senior manager that left reported to the replacement senior manager. When the appointed senior manager left, the replacement senior manager had already been on staff and at no point during the duration of this issue was Texas RE_URE3's NERC internal compliance program (ICP) left without leadership. In addition, Texas RE_URE3 is a small entity and all of its employees involved in NERC compliance knew at all times who was responsible for Texas RE_URE3's NERC ICP. Also, Texas RE_URE3 submitted an attestation that it did not have any Critical Assets during the time period of this issue.	Texas RE_URE3's internal cyber security procedure was updated to include the new single senior manager. The manager at the facility location and the compliance employees are aware of the updated document and its location, and have access to the document.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (Texas RE_URE4) Nueces Bay WLE LP (Nueces Bay)	NCRXXXXX	TRE201100522	CIP-003-3	R2.2	Texas RE_URE4 self-reported that its appointed single senior manager with overall responsibility and authority for leading and managing Texas RE_URE4 implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3, left the company. Texas RE_URE4's CIP procedure identifying this senior manager was not updated within 30 days of his departure, which presented an issue with CIP-003-3 R2.2. TRE determined that the issue duration was approximately four months, 30 days after the manager left, until Texas RE_URE4's internal compliance procedure was updated.	This issue did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS). TRE determined that based on the administrative nature of this issue, the availability of responsible leadership throughout the period, and Texas RE_URE4's lack of Critical Assets, the risk to the reliability of the BPS was minimal. First, the senior manager that left reported to the replacement senior manager. When the appointed senior manager left, the replacement senior manager had already been on staff and at no point during the duration of this issue was Texas RE_URE4's NERC internal compliance program (ICP) left without leadership. In addition, Texas RE_URE4 is a small entity and all of its employees involved in NERC compliance knew at all times who was responsible for Texas RE_URE4's NERC ICP. Also, Texas RE_URE4 submitted an attestation that it did not have any Critical Assets during the time period of this issue.	Texas RE_URE4's internal cyber security procedure was updated to include the new single senior manager. The manager at the facility location and the compliance employees are aware of the updated document and its location, and have access to the document.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2011008650	CIP-007-3	R6	WECC_URE1 submitted a Self-Report stating that non-critical Cyber Assets were added to an Electronic Security Perimeter (ESP). The Cyber Assets were not configured to send Security Status Monitoring alerts to the syslog server. WECC_URE1 reported that consequently, access logs were not maintained nor reviewed per CIP-007-3 R6. WECC reviewed WECC_URE1's Self-Report and determined that WECC_URE 1 expanded its ESP to include non-critical Cyber Assets. WECC determined that WECC_URE1 failed to ensure these non-critical Cyber Assets were configured to send syslogs to its centralized server. WECC, therefore, determined that WECC_URE1 failed to ensure all Cyber Assets within the ESP implemented automated tools to monitor system events after expanding the boundary of an ESP.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. The scope of the issue is limited to 18% of the non-critical Cyber Assets within the ESP. All Cyber Assets including the non-critical Cyber Assets within scope of the issue addressed herein were secured behind a firewall through which electronic access was controlled, logged and monitored. Further, although the non-critical Cyber Assets were not configured to log system events with the centralized server, the non-critical Cyber Assets did maintain logs locally that could have been reviewed if a threat was detected. All Cyber Assets were located within a Physical Security Perimeter. Personnel with electronic or physical access to devices completed Personnel Risk Assessments and Cyber Security Training.	WECC_URE1 reconfigured the non-critical Cyber Assets devices within the ESP to ensure that cyber security event logs were centrally maintained and reviewed.

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 Electric Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012009098	CIP-004-3	R4	WECC_URE2 submitted a Self-Report reporting one instance in which specific access rights to Critical Cyber Assets (CCAs) were not listed and, one instance in which access rights were not revoked within seven days for personnel who no longer required such access. The first issue reported by WECC_URE2 occurred after WECC_URE2 implemented a configuration change. After the configuration change was made, access lists reflected that one individual maintained electronic access to one CCA when, in fact, the individual maintained electronic access rights to a total of six CCAs. WECC_URE2 detected the problem and revised its access list to include all of the individual's access rights to the six CCAs. WECC_URE2 access lists, therefore, failed to list specific access rights as required under CIP-004-3 R4 for one individual. The second issue reported by WECC_URE2 stemmed from its failure to revoke physical access within seven days for a single person who no longer required such access. The individual was an intern with physical access rights to CCAs located within the control center. The internship ended but the individual's security badge, provisioning physical access to the control room, was not returned until ten days later. Because the badge was not turned in within seven days of the intern's departure, WECC determined that WECC_URE2 failed to comply with CIP-004 R4.2 for a period of three days.	This issue posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system. Each of the two individuals within scope of the issue described herein completed Personnel Risk Assessments and Cyber Security Training. Further, WECC_URE2 remediated both instances upon detection. WECC_URE2 revised access lists to include specific electronic access rights held by one individual and, WECC_URE2 revoked physical access within ten days of the other individual's departure. All CCAs to which individuals had access were secured within Physical Security Perimeters and Electronic Security Perimeters. All electronic and physical access to these CCAs was logged and monitored.	WECC_URE2 has undertaken a number of mitigating activities to address immediate instances and to prevent future reoccurrence. WECC_URE2 revised access lists to include all electronic access rights maintained by the individual in scope of the issue. WECC_URE2 is base-lining the access management system for appropriate CIP devices and all user accounts. WECC_URE2 implemented a manual process whereby the current user accounts/access privileges can still be reviewed and validated each quarter. WECC_URE2 implemented the use of additional reports that highlight updates associated with adding/changing or removing CIP devices and/or accounts. WECC_URE2 revoked access rights for the intern. WECC_URE2 is implementing training requirements to ensure that managers revoke physical access within the timeframe prescribed under R4.2.

Document Accession #: 20120530-5260 Filed Date: 05/30/2012

Document Content(s)