Federal Energy Regulatory Commission
Washington, D.C. 20426

January 13, 2022

FOIA No. FY19-30 (RC12-15)
Forty Ninth 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 November 22, 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. RC12-15, along with the names of ten (10) relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] Based on my own review of the relevant documents, including comments submitted by certain UREs, I conclude that disclosure of these URE identities is appropriate and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC12-15.

With respect to the remaining identities of UREs contained in RC12-15, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the

[1] 5 U.S.C. § 552 (2018).

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

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-15 will not be disclosed.

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

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

Sincerely,

BENJAMIN WILLIAMS

Digitally signed by BENJAMIN WILLIAMS
Date: 2022.01.13 14:44:41 -05'00'

Benjamin Williams
Deputy Director
Office of External Affairs

Enclosure

cc:

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

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

August 31, 2012

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

Re: NERC FFT Informational Filing
FERC Docket No. RC12-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find, Fix, Track and Report[1] (FFT) in Attachment A regarding 38 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 62 possible violations[5] of 14 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 62 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is 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, Track and 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 Charles A. Berardesco* Senior Vice President, General Counsel, and Corporate Secretary North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 charles.berardesco@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

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

cc: Entities listed in Attachment B

NERC

Attachment a

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

Attachment b

Additions to the service list

ATTACHMENT B

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

FOR FRCC:

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

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

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

FOR MRO:

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

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

FOR NPCC:

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

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

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

FOR RFC:

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

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

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

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

FOR SERC:

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

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

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

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

FOR SPP RE:

Ron Ciesiel*
General Manager
Southwest Power Pool Regional Entity
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

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

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

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
August 31, 2012

Take notice that on August 31, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty-eight (38) 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)	Florida Power & Light Co. (FPL)	NCR00024	FRCC2012010060	PRC-005-1a	R2	On April 11, 2012, FPL, as a Transmission Owner, self-reported an issue with PRC-005-1a R2. During an internal review of FPL's Protection System maintenance and testing program, maintenance for a single transmission substation battery bank was identified as having a completion date which was past the interval-based due date by four days. Maintenance on the battery bank at issue should have been completed on September 30, 2011 and was actually completed on October 4, 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 the batteries were continuously monitored and an alarm would have alerted FPL personnel in case of a voltage issue or an open battery bank. Additionally, the battery bank was only four days overdue for testing and maintenance. When tested, the batteries were found to be fully functional. Although FPL has violated this Standard previously, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation. The prior violation occurred in 2007, in the early stages of mandatory compliance. In 2007, FPL failed to maintain and/or test a number of devices on the intervals required by its maintenance and testing program because of a computer tracking error and a misunderstanding of program flexibility regarding coordination with generator schedules and equipment outages. Following the prior violation, FPL improved its processes and computer software. The instant remediated issue was an isolated event caused by insufficient training of contractors and/or personnel and does not represent a reoccurrence of the previous noncompliance.	To mitigate this issue, FPL tested and maintained the battery bank that was out of interval, and trained the contractor and FPL personnel on the procedure and necessity for on-time maintenance.
Reliability*First* Corporation (Reliability*First*)	Cambria CoGen Company (CCC)	NCR00705	RFC2012009873	FAC-008-1	R1	From January 23, 2012 through February 3, 2012, Reliability*First* conducted a compliance audit of CCC (Compliance Audit). During the Compliance Audit, Reliability*First* determined that CCC, as a Generator Owner, had an issue with FAC-008-1 R1 for failing to document a methodology to determine Facility Ratings for its 115 kV transmission line that interconnects CCC's generator facility with Pennsylvania Electric Company's (PENELECs') substation. CCC had an agreement to supply power to PENELEC until March 2011.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that CCC's 115 kV transmission line is not the most limiting component at the CCC generating facility. The most limiting components at the CCC generating facility are the turbine gearbox and generator. Therefore, CCC's generator would have tripped off line due to exceeding the maximum capability of the turbine gearbox before CCC would have exceeded the maximum capability of its 115 kV line. There are no records to indicate that the operation of CCC's generator has ever been limited by the 115 kV line or that CCC's generator has ever tripped off line or been separated from the BPS due to a failure or malfunction of CCC's 115 kV transmission line during the generator's 21 years of operation (CCC acquired the facility in 2004).	CCC documented a methodology and associated Facility Rating for its 115 kV transmission line.
Reliability*First* Corporation (Reliability*First*)	Cambria CoGen Company (CCC)	NCR00705	RFC2012009874	FAC-009-1	R1	From January 23, 2012 through February 3, 2012, Reliability*First* conducted a compliance audit of CCC (Compliance Audit). During the Compliance Audit, Reliability*First* determined that CCC, as a Generator Owner, had an issue with FAC-009-1 R1 for failing to establish Facility Ratings for its protective relay equipment based on its Facility Ratings Methodology. According to its Methodology, CCC should have included Facility Ratings consistent with "manufacturer's published ratings, or … based upon industry rating practices such as manufacturer's warranty, IEEE, ANSI or other applicable standards" for its protective relay equipment. CCC included its protective relay settings, not manufacturer's published ratings or ratings based on industry rating practices, as its protective relay equipment in its Facility Ratings Methodology. CCC's use of these settings was not consistent with the associated Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that CCC included protective relay settings, which were within the manufacturer's ratings, in its Facility Ratings Methodology. Therefore, the relay settings used by CCC provided a more restrictive parameter than the manufacturer's ratings. Additionally, the most limiting components at the CCC generating facility are the turbine gearbox and generator. Therefore, CCC's generator would have tripped off line due to exceeding the maximum capability of the turbine gearbox before CCC would have exceeded either the protective relay settings or the manufacturer's ratings for CCC's protective relays. CCC's use of relay settings as opposed to manufacturer's ratings did not limit the generation output of CCC during the duration of the issue.	CCC revised the ratings for all its protective relays to be consistent with its Facility Ratings Methodology and re-evaluated and revised, when necessary, its Facility Ratings based on its revised protective relay Facility Ratings.

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*)	Cambria CoGen Company (CCC)	NCR00705	RFC2012009875	PRC-005-1	R1	From January 23, 2012 through February 3, 2012, Reliability*First* conducted a compliance audit of CCC (Compliance Audit). During the Compliance Audit, Reliability*First* determined that CCC, as a Generator Owner, had an issue with PRC-005-1 R1 because its Protection System maintenance and testing program (Program) did not include maintenance and testing intervals for its current and voltage sensing devices, DC control circuitry or station batteries (CCC has no associated communication systems). Further, CCC did not provide a basis for the maintenance and testing intervals of its relays. Finally, CCC did not include a summary of maintenance and testing procedures in its Program for any of its Protection System devices.	Reliability*First* determined that this issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that this issue was a result of a documentation error. While CCC's Program was deficient, its maintenance and testing practices were not. During the duration of the issue, CCC used the *2001 InterNational Electrical Testing Association Maintenance Testing Specifications* manual (NETA Manual) as the basis for the maintenance and testing of its Protection System devices. For clarification, the NETA Manual and CCC's Program are not the same document. The NETA Manual included tests and intervals for each of CCC's Protection System devices. CCC was performing, through an outside firm, maintenance and testing for its Protection System devices pursuant to the NETA Manual, but did not have all the Protection System components and the related tests, intervals, and bases for those intervals set forth in its own Program. In addition, during the Compliance Audit, CCC provided Reliability*First* with maintenance and testing records demonstrating that maintenance and testing was performed on all its Protection System devices during the duration of the issue with PRC-005-1 R1. During the Compliance Audit, CCC did provide Reliability*First* with the previous and last maintenance and test records for all the requested Protection System devices.	CCC revised its Program to include intervals for current and voltage sensing devices, DC control circuitry and station batteries. CCC also included the basis for the intervals associated with its Protection System devices as well as a summary of maintenance and testing procedures in its Program.
SERC Reliability Corporation (SERC)	LSP Energy Limited Partnership (LSP Energy)	NCR01266	SERC201100760	PRC-005-1	R2	On February 21, 2011, LSP Energy, as a Generator Owner (GO) and Transmission Owner (TO), self-reported an issue with PRC-005-1 R2, stating that as part of its Protection System maintenance and testing program for batteries, LSP Energy performs monthly, quarterly, annual and five-year testing. During an internal compliance review conducted during the week of January 24, 2011, LSP Energy could not locate the records for the monthly battery maintenance for five batteries in October 2010. SERC staff requested and reviewed spreadsheets prepared by LSP Energy that included each of LSP Energy'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 assigned intervals based on a review of LSP Energy's Protection System maintenance and testing procedure for its GO and TO functions. In addition to the missed monthly battery maintenance for all five batteries in October 2010, SERC staff determined that LSP Energy also missed the required monthly battery maintenance for four batteries in January 2009 and one battery in October 2009. SERC staff determined that LSP Energy failed to have documentation that five batteries (100% of the total) were maintained and tested within the defined intervals. Noncompliance was limited to three non-consecutive monthly maintenance intervals for the five batteries. In total, LSP Energy failed to have documentation that its Protection System devices were maintained and tested within the defined intervals for five of its 133 Protection System devices (approximately 3.8%).	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. LSP Energy is manned 24 hours a day. Twice a day, once per shift, LSP Energy personnel visually inspect the batteries during operator rounds; 2. The battery chargers have alarms designed to alert personnel in the event of a malfunction. No alarms went off during the time of the issue; 3. LSP Energy found no deficiencies when it completed the battery maintenance and testing during the maintenance periods before and after the missed monthly maintenance; and 4. LSP Energy missed battery maintenance inspections in non-consecutive months. Of the missed inspections, LSP Energy missed three monthly inspections for one battery, two monthly inspections for three batteries, and one monthly inspection for one battery.	SERC verified that LSP Energy completed the following actions: 1. Created an electronically generated monthly preventative maintenance that requires compliance personnel to conduct an internal audit of the timeliness and completeness of battery testing and maintenance records; 2. Held NERC regulatory training, including Protection System maintenance and testing intervals for all plant employees, which will be repeated annually; 3. Revised its procedure for testing schedule intervals for batteries to specify the interval and grace period for monthly, quarterly, annual, and five-year testing, as well as specific tests to conduct in each interval period; and 4. Posted battery maintenance and testing summary charts in the Compliance office and Instrument, Control & Electrician office that provide a visual summary that battery maintenance and testing has been completed on a timely basis.
SERC Reliability Corporation (SERC)	USACE - Charleston District (USACE - Charleston)	NCR01356	SERC200800152	FAC-009-1	R1	On June 30, 2008, USACE - Charleston, as a Generator Owner, self-certified an issue with FAC-009-1 R1, stating that it did not have a documented Facility Rating Methodology (FRM) and therefore could not confirm that its Facility Ratings were consistent with an associated FRM.	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 because: 1. At the time of the issue, USACE - Charleston had established and published Facility Ratings consistent with the design criteria; and 2. The Facilities were operated within those design criteria.	SERC verified that USACE - Charleston completed the following actions: Developed a FRM and in accordance with it has: 1. Compiled data for each element comprising a facility; 2. Reviewed compiled data for inconsistencies and errors, and mitigated any such inconsistencies or errors; 3. Analyzed the compiled data to determine the most limiting element within a facility; and 4. Documented the most limiting element and the overall ratings for each facility.

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)	USACE - Charleston District (USACE - Charleston)	NCR01356	SERC200800153	PRC-005-1	R1	On June 30, 2008, USACE - Charleston, as a Generator Owner, self-certified an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program failed to include: 1. Intervals for batteries and DC control circuits; 2. A basis for intervals for batteries and DC control circuits, or for relays, communication systems, and current and potential sensing devices; and 3. A summary description of the maintenance and testing procedures.	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 because: USACE - Charleston provided evidence in the form of dated records of maintenance and testing, manufacturers' recommendations, maintenance and testing procedures, and corporate policies to show that all components of the Protection System were being maintained and tested on a regular basis despite lacking the required level of documentation in its Protection System maintenance and testing program.	SERC verified that USACE - Charleston completed the following actions: The USACE South Atlantic Division, of which USACE - Charleston is a part, has: 1. Revised its Protection System maintenance and testing program to include the basis for the maintenance and testing interval for its Protective System devices; 2. Revised its Protection System maintenance and testing program to include a summary of its maintenance and testing procedures for its Protective System devices; and 3. Reviewed, approved and implemented the revised Protection System maintenance and testing program.
SERC Reliability Corporation (SERC)	USACE - Charleston District (USACE - Charleston)	NCR01356	SERC200800154	FAC-008-1	R1	On June 30, 2008, USACE - Charleston, as a Generator Owner, self-certified an issue with FAC-008-1 R1, stating that it had not documented its historical method of determining Facility Ratings.	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 because: 1. USACE - Charleston had a historical method of determining Facility Ratings based on design parameters, nameplate ratings, other operational limits determined by the manufacturers, and utilized good engineering practice; and 2. USACE - Charleston had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue, making the determined ratings credible.	SERC verified that USACE - Charleston completed the following actions: The USACE South Atlantic Division, of which USACE - Charleston is a part, has developed a Facility Ratings Methodology.
SERC Reliability Corporation (SERC)	USACE - Mobile District (USACE - Mobile)	NCR01359	SERC200800145	FAC-008-1	R1	On June 19, 2008, USACE - Mobile, as a Generator Owner, self-certified an issue with FAC-008-1 R1, stating that it had not documented its historical method of determining Facility Ratings.	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 because: 1. USACE - Mobile had a historical method of determining Facility Ratings based on design parameters, nameplate ratings, other operational limits determined by the manufacturers, and utilized good engineering practice; and 2. USACE - Mobile had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue, making the determined ratings credible.	SERC verified that USACE - Mobile completed the following actions: The USACE South Atlantic Division, of which USACE - Mobile is a part, has developed a Facility Ratings Methodology.
SERC Reliability Corporation (SERC)	USACE - Mobile District (USACE - Mobile)	NCR01359	SERC200800146	FAC-009-1	R1	On June 19, 2008, USACE - Mobile, as a Generator Owner, self-certified an issue with FAC-009-1 R1, stating that it did not have a documented Facility Rating Methodology (FRM) and therefore could not confirm that its Facility Ratings were consistent with an associated FRM.	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 because: USACE - Mobile had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue.	SERC verified that USACE - Mobile completed the following actions: Developed a FRM and in accordance with it has: 1. Compiled data for each element comprising a facility; 2. Reviewed compiled data for inconsistencies and errors, and mitigated any such inconsistencies or errors; 3. Analyzed the compiled data to determine the most limiting element within a facility; and 4. Documented the most limiting element and the overall ratings for each facility.
SERC Reliability Corporation (SERC)	USACE - Mobile District (USACE - Mobile)	NCR01359	SERC200800147	PRC-005-1	R1	On June 19, 2008, USACE - Mobile, as a Generator Owner, self-certified an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program failed to include: 1. Intervals for batteries and DC control circuits; 2. A basis for intervals for batteries and DC control circuits, or for relays, communication systems, and current and potential sensing devices; and 3. A summary description of the maintenance and testing procedures.	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 because: USACE - Mobile provided evidence in the form of dated records of maintenance and testing, manufacturers' recommendations, maintenance and testing procedures, and corporate policies to show that all components of the Protection System were being maintained and tested on a regular basis despite lacking the required level of documentation in its Protection System maintenance and testing program.	SERC verified that USACE - Mobile completed the following actions: The USACE South Atlantic Division, of which USACE - Mobile is a part, has: 1. Revised its Protection System maintenance and testing program to include the basis for the maintenance and testing interval for its Protective System devices; 2. Revised its Protection System maintenance and testing program to include a summary of its maintenance and testing procedures for its Protective System devices; and 3. Reviewed, approved and implemented the revised Protection System maintenance and testing program.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	USACE - Savannah District (USACE - Savannah)	NCR01361	SERC200800158	FAC-008-1	R1	On July 7, 2008, USACE - Savannah, as a Generator Owner, self-certified an issue with FAC-008-1 R1, stating that it had not documented its historical method of determining Facility Ratings.	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 because: 1. USACE - Savannah had a historical method of determining Facility Ratings based on design parameters, nameplate ratings, other operational limits determined by the manufacturers, and utilized good engineering practice; and 2. USACE - Savannah had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue, making the determined ratings credible.	SERC verified that USACE - Savannah completed the following actions: The USACE South Atlantic Division, of which USACE - Savannah is a part, has developed a Facility Ratings Methodology.
SERC Reliability Corporation (SERC)	USACE - Savannah District (USACE - Savannah)	NCR01361	SERC200800159	FAC-009-1	R1	On July 7, 2008, USACE - Savannah, as a Generator Owner, self-certified an issue with FAC-009-1 R1, stating that it did not have a documented Facility Rating Methodology (FRM) and therefore could not confirm that its Facility Ratings were consistent with an associated FRM.	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 because: USACE - Savannah had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue.	SERC verified that USACE - Savannah completed the following actions: Developed a FRM and in accordance with it has: 1. Compiled data for each element comprising a facility; 2. Reviewed compiled data for inconsistencies and errors, and mitigated any such inconsistencies or errors; 3. Analyzed the compiled data to determine the most limiting element within a facility; and 4. Documented the most limiting element and the overall ratings for each facility.
SERC Reliability Corporation (SERC)	USACE - Savannah District (USACE - Savannah)	NCR01361	SERC200800160	PRC-005-1	R1	On July 7, 2008, USACE - Savannah, as a Generator Owner, self-certified an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program failed to include: 1. Intervals for batteries and DC control circuits; 2. A basis for intervals for batteries and DC control circuits, or for relays, communication systems, and current and potential sensing devices; and 3. A summary description of the maintenance and testing procedures.	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 because: USACE - Savannah provided evidence in the form of dated records of maintenance and testing, manufacturers' recommendations, maintenance and testing procedures, and corporate policies to show that all components of the Protection System were being maintained and tested on a regular basis despite lacking the required level of documentation in its Protection System maintenance and testing program.	SERC verified that USACE - Savannah completed the following actions: The USACE South Atlantic Division, of which USACE - Savannah is a part, has: 1. Revised its Protection System maintenance and testing program to include the basis for the maintenance and testing interval for its Protective System devices; 2. Revised its Protection System maintenance and testing program to include a summary of its maintenance and testing procedures for its Protective System devices; and 3. Reviewed, approved, and implemented the revised Protection System maintenance and testing program.
SERC Reliability Corporation (SERC)	USACE - Wilmington District (USACE - Wilmington)	NCR01364	SERC200800166	FAC-008-1	R1	On July 14, 2008, USACE - Wilmington, as a Generator Owner, self-certified an issue with FAC-008-1 R1, stating that it had not documented its historical method of determining Facility Ratings.	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 because: 1. USACE - Wilmington had a historical method of determining Facility Ratings based on design parameters, nameplate ratings, other operational limits determined by the manufacturers, and utilized good engineering practice; and 2. USACE - Wilmington had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue, making the determined ratings credible.	SERC verified that USACE - Wilmington completed the following actions: The USACE South Atlantic Division, of which USACE - Wilmington is a part, has developed a Facility Ratings Methodology.
SERC Reliability Corporation (SERC)	USACE - Wilmington District (USACE - Wilmington)	NCR01364	SERC200800167	FAC-009-1	R1	On July 14, 2008, USACE - Wilmington, as a Generator Owner, self-certified an issue with FAC-009-1 R1, stating that it did not have a documented Facility Rating Methodology (FRM) and therefore could not confirm that its Facility Ratings were consistent with an associated FRM.	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 because: USACE - Wilmington had established and published Facility Ratings that were consistent with the station output as it was operated at the time of the issue.	SERC verified that USACE - Wilmington completed the following actions: Developed a FRM and in accordance with it has: 1. Compiled data for each element comprising a facility; 2. Reviewed compiled data for inconsistencies and errors, and mitigated any such inconsistencies or errors; 3. Analyzed the compiled data to determine the most limiting element within a facility; and 4. Documented the most limiting element and the overall ratings for each facility.

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)	USACE - Wilmington District (USACE - Wilmington)	NCR01364	SERC200800168	PRC-005-1	R1	On July 14, 2008, USACE - Wilmington, as a Generator Owner, self-certified an issue with PRC-005-1 R1, stating that its Protection System maintenance and testing program failed to include: 1. Intervals for batteries and DC control circuits; 2. A basis for intervals for batteries and DC control circuits, or for relays, communication systems, and current and potential sensing devices; and 3. A summary description of the maintenance and testing procedures.	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 because: USACE - Wilmington provided evidence in the form of dated records of maintenance and testing, manufacturers' recommendations, maintenance and testing procedures, and corporate policies to show that all components of the Protection System were being maintained and tested on a regular basis despite lacking the required level of documentation in its Protection System maintenance and testing program.	SERC verified that USACE - Wilmington completed the following actions: The USACE South Atlantic Division, of which USACE - Wilmington is a part, has: 1. Revised its Protection System maintenance and testing program to include the basis for the maintenance and testing interval for its Protective System devices; 2. Revised its Protection System maintenance and testing program to include a summary of its maintenance and testing procedures for its Protective System devices; and 3. Reviewed, approved, and implemented the revised Protection System maintenance and testing program.
Southwest Power Pool Regional Entity (SPP RE)	Mississippi Delta Energy Agency (MDEA)	NCR06050	SPP2011008070	PRC-023-1	R1;R1.1	On September 8, 2011, MDEA, as a Transmission Owner, self-reported noncompliance with PRC-023-1 R1.1. MDEA reported that one of its two load-responsive phase protection systems (its SEL311C relay) was not set in accordance with the criteria set forth in R1.1 through R1.13 of PRC-023-1. The SEL311C relay should have been set to operate when the line loading was 1,350 Amps, 150% of the highest seasonal Facility Rating of a applicable circuit, for the available defined loading duration nearest 4 hours. During the period of July 1, 2010, through June 8, 2011, the SEL311C relay was set to operate when its line loading was 1,343 Amps, 7 Amps below the Amp setting required by R1.1.	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). MDEA owns a single 23 mile 230 kV transmission line. Although the SEL311C relay's incorrect setting could have resulted in a premature trip of MDEA's 230 kV transmission line, the trip would have occurred based upon a line loading within less than 1% of the amp setting required by R1.1. The difference in the setting is de minimis and would not have substantively limited the loadability of the MDEA transmission line or interfered with the relay's protection of the MDEA transmission line from a fault.	MDEA modified the incorrect relay setting to comply with the criterion described in PRC-023-1 R1.1. SPP RE verified completion of the mitigating activities.
Southwest Power Pool Regional Entity (SPP RE)	Noble Great Plains Windpark, LLC (Noble GP)	NCR11070	SPP2012009358	CIP-001-1	R1	On January 20, 2012, Noble GP, as a Generator Operator, self-certified noncompliance with CIP-001-1 R1. Noble GP did not have a procedure for recognizing and making operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection, which presented an issue with CIP-001-1 R1.	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 Noble GP did not have a procedure for recognizing sabotage and making operating personnel aware of sabotage events on its facilities and multi-sabotage affecting larger portions of the Interconnection, it did have an Emergency Response Policy that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid, that could occur as a result of sabotage. The Emergency Response Policy was disseminated to all personnel at the wind facility. Furthermore, Noble GP is a wind-powered variable energy facility with a maximum capacity of 114 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the interconnection. The size and scope of its facilities, coupled with its implemented Emergency Response Policy, reduce the risk from Noble GP's failure to have a procedure for recognizing and making operating personnel aware of sabotage events to minimal.	Noble GP has implemented a procedure for the recognition of and making operating personnel aware of sabotage events.
Southwest Power Pool Regional Entity (SPP RE)	Noble Great Plains Windpark, LLC (Noble GP)	NCR11070	SPP2012009359	CIP-001-1	R2	On January 20, 2012, Noble GP, as a Generator Operator, self-certified noncompliance with CIP-001-1 R2. Noble GP did not have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection, which presented an issue with CIP-001-1 R2.	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 Noble GP did not have a procedure for recognizing sabotage or communicating information concerning sabotage to appropriate parties in the Interconnection, it did have an Emergency Response Policy that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid, that could occur as a result of sabotage. Also, this Emergency Response Policy did have directions to notify members of the Interconnect in case of an emergency. The Emergency Response Policy was disseminated to all personnel at the wind facility. Furthermore, Noble GP is a wind-powered variable energy facility with a maximum capacity of 114 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the interconnection. The size and scope of its facilities, coupled with its implemented Emergency Response Policy, reduce the risk from Noble GP's failure to have a procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection to minimal.	Noble GP has implemented a procedure for the recognition of sabotage, and the communication of information concerning sabotage to appropriate parties in the Interconnection.

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)	Noble Great Plains Windpark, LLC (Noble GP)	NCR11070	SPP2012009360	CIP-001-1	R3	On January 20, 2012, Noble GP, as a Generator Operator, self-certified noncompliance with CIP-001-1 R3. Noble GP did not have sabotage response guidelines for reporting sabotage related disturbances, and therefore could not provide such guidelines to its operating personnel, which presented an issue with CIP-001-1 R3.	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 Noble GP did not have sabotage response guidelines for reporting disturbances due to sabotage and therefore could not provide such guidelines to its operating personnel, it did have an Emergency Response Policy that raised awareness for many emergencies, including turbine equipment failure, detection of fires, and other events that would significantly affect the delivery of electricity to the grid, that could occur as a result of sabotage, as well as response guidelines for reporting those emergencies. The Emergency Response Policy was disseminated to all personnel at the wind facility. Furthermore, Noble GP is a wind-powered variable energy facility with a maximum capacity of 114 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the interconnection. The size and scope of its facilities, coupled with its implemented Emergency Response Policy, reduce the risk from Noble GP's failure to provide a sabotage response guidelines to its operating personnel to minimal.	Noble GP has implemented sabotage response guidelines for reporting disturbances due to sabotage, which Noble GP provided to its operating personnel.
Southwest Power Pool Regional Entity (SPP RE)	Noble Great Plains Windpark, LLC (Noble GP)	NCR11070	SPP2012010689	CIP-001-1	R4	On July 12, 2012, Noble GP, as a Generator Operator, self-reported noncompliance with CIP-001-1 R4. Noble GP did not establish communication contacts with local Federal Bureau of Investigation (FBI) officials or that it had developed reporting procedures as appropriate to its circumstances, which presented an issue with CIP-001-1 R4.	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 Noble GP did not have established communication contacts with local FBI officials or developed reporting procedures appropriate to its circumstances, it did have an Emergency Response Policy which included contacts for local law enforcement officials, including local police department, fire station, and hospital officials. Furthermore, Noble GP is a wind-powered variable energy facility with a maximum capacity of 114 MW. Its variable output prevents the facility from being dispatched to support base load or being deemed critical generation within the interconnection. The size and scope of its facilities, coupled with its implemented Emergency Response Policy, reduce the risk from Noble GP's failure to have established contact with the FBI and developed reporting procedures as appropriate to its circumstances to minimal.	Noble GP has implemented a written procedure for the communication of information regarding sabotage events to the FBI per CIP 001 R4.
Texas Reliability Entity, Inc. (Texas RE)	Nueces Bay WLE LP (Nueces Bay)	NCR04106	TRE201100514	VAR-002-1.1b	R3.1	On October 25, 2011, Nueces Bay, as a Generator Operator, filed a Self-Report of VAR-002-1.1b R3.1. On June 4, 2011, Nueces Bay's 223 MVA unit was brought off line due to exciter problems. Because the exciter was powered down to replace a bad card and fan motor, the unit operator was required to manually enable the Power System Stabilizer (PSS) to function automatically during future starts. However, the unit operator did not manually enable the PSS function. On the subsequent unit restarts on June 4, June 5 and June 6, 2011, the PSS remained in the "Disable" mode. The operators did not notice the alarm indicating the PSS was not "Enabled." As a result, Nueces Bay failed to report the status change on the unit to the Transmission Operator (TOP) as soon as practical, nor within 30 minutes, as required in VAR-002-1.1b R3.1. The issue was discovered at approximately 14:30 hours on Monday, June 6, 2011 and the PSS operating mode was changed to "Enabled." On June 9, 2011 the Qualified Scheduling Entity, which communicates with the TOP, was notified regarding the PSS status issue and the Qualified Scheduling Entity then reported the status change to the TOP. Texas RE determined that Nueces Bay had an issue with this standard from June 4, 2011, when the unit operator did not enable the PSS to function automatically, to June 9, 2011, when the status change was reported to the TOP.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the unit was run for 31 hours with a disabled PSS and the Automatic Voltage Regulation (AVR) system was online for all of the unit's run hours, reducing the probability of system instability. The AVR system ensured that the unit could effectively respond to any system voltage deviations even when the PSS was functioning on the "Disabled" mode. Finally, the size of the unit was 223 MVA, thereby further reducing the risk to the BPS.	Nueces Bay took the following actions to mitigate this issue: 1. Conducted an all-hands meeting-and reminded operators of the VAR-002 compliance obligations; 2. Revised its Start-up Check List to include instructions requiring that the PSS be enabled; 3. Created a new shift turnover log that includes instructions to visually inspect / walk down the control boards and to discuss any new or unusual alarms; 4. Posted training, *Generator Operation for Maintaining Network Voltage Schedules* on the company's Learning Management site and listed it as required training for operators; 5. Revised the Start-up Check List to include instructions for operators to ensure the AVR is in auto and controlling voltage in the voltage control mode; 6. Configured the control screens to include a pop-up dialog box that appears whenever an operator attempts to change the PSS or AVR status. The dialog box includes a reminder statement about TOP notification whenever status is changed and requires user acknowledgement before allowing a status change. Texas RE verified completion of these mitigation activities.

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)	Lower Colorado River Authority (LCRA)	NCR04092	TRE2012009904	VAR-002-1.1b	R3.1	LCRA, as a Generator Operator, self-reported that it had a remediated issue of VAR-002-1.1b R3.1. LCRA failed to notify its Transmission Operator (TOP) within 30 minutes of the Automatic Voltage Regulation (AVR) status change for its Gideon Unit 2 that occurred on January 23, 2012 from 10:45 to 15:20. LCRA did not notify the TOP either verbally or by email of the first AVR status change that occurred on January 23, 2012 from 10:45 to 15:20. In addition, LCRA self-reported it had a second instance of noncompliance because it failed to notify its TOP of a Gideon Unit 2 AVR status change within 30 minutes. The second status change occurred at 16:35 on January 23, 2012. However, LCRA did notify its TOP approximately 12 hours after the second Gideon Unit 2 AVR status change that occurred at 16:35 on January 23, 2012. The Electric Reliability Council of Texas (ERCOT) serves as LCRA's TOP for the purpose of complying with this Standard. Although as a TOP, ERCOT, was notified immediately by LCRA's real-time telemetry of the two status changes, the operating desk at LCRA did not notify ERCOT either verbally or by email within 30 minutes of the two changes in AVR status at Gideon Unit 2 or of the expected duration of the changes in status, as required by VAR-002-1.1b R3.1 and by LCRA's internal procedures. The operating desk, called GenDesk, notified LCRA's System Operations Control Center, by phone, at approximately 06:45 on January 24, 2012. TRE determined that the duration of the first issue was from 11:15 to 15:20 on January 23, 2012 and the duration of the second issue was from 17:05 on January 23, 2012 to 06:45 on January 24, 2012.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the TOP was not notified of the two AVR status changes and their duration within 30 minutes, the information was telemetered in real-time to the TOP. Therefore, the TOP was aware of the status changes immediately but was not aware of the duration of the status changes. Texas RE also considered the size of the unit at issue, which had 200 MW of capacity. In addition, LCRA had a process in place instructing operators to notify the TOP of status changes but the operators failed to follow the process properly. Section 2.1.2 of LCRA's Maintaining Network Voltage process states that the GenDesk will inform ERCOT and LCRA's System Operations Control Center of AVR failure and expected duration of failure. The process does state that AVR and Power System Stabilizer (PSS) status is automatically telemetered to ERCOT but also calls for verbal notification to be performed within 30 minutes.	LCRA took multiple actions to mitigate the reported issue and prevent recurrence. Those actions included the following: 1. LCRA sent emails to both the generation facility control room operators and to the GenDesk operators. The email to the generation facility control room operators included a reminder that GenDesk must be contacted within 30 min of a change of AVR or PSS Status. The GenDesk operators were reminded via email that ERCOT and LCRA's Transmission Service Provider must be contacted within 30 minutes of change of status to AVR or PSS. 2. LCRA GenDesk added "AVR out of Service" indicators to the Generation Management System (GMS) which is the primary display the GenDesk traders utilize. 3. All generation facilities installed an additional alarm description to their distributed control systems (DCS) that directs operators to inform the GenDesk when AVR trips to manual mode. 4. The Compliance Department made improvements to the Maintaining Network Voltage process to prevent recurrence of instances of noncompliance. Texas RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc. (Texas RE)	Edison Mission Marketing & Trading, Inc. (EMMT)	NCR00769	TRE201100480	FAC-008-1	R1.3	During a October 4, 2011 to October 7, 2011 Audit of EMMT, Texas RE discovered that the Facility Rating Methodology (FRM) in place since EMMT became a registered Generator Owner (GO) on May 28, 2008, did not reference consideration of design criteria, ambient conditions and operating limitations, as required by FAC-008-1 R1.3. EMMT had included those considerations when engineering its generating facilities and this was substantiated by the engineering and design documentations EMMT provided to Texas RE. Prior to the Audit, on August 24, 2011, EMMT amended its FRM to address the requirements of FAC-008-1 R1.3. Texas RE determined that the remediated issue was from May 28, 2008, when EMMT registered as a GO, through August 24, 2011, when EMMT amended its FRM.	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, even though EMMT did not state its consideration of design criteria, ambient conditions, or operating limitations in its original FRM, EMMT did in fact have documents on file to substantiate application of those principles in the construction of its generating facilities. Texas RE determined that the operability and reliability of its systems was never affected by this omission in EMMT's FRM.	EMMT promptly amended its FRM to include language to address the requirements of FAC-008-1 R1.3. No other actions were necessary as EMMT demonstrated, through documentation, that they were already performing the related tasks as part of its standard practices. Texas RE verified completion of the mitigation activities.
Western Electricity Coordinating Council (WECC)	Bonneville Power Administration (BPA)	NCR05032	WECC201102885	MOD-029-1a	R2.6	On July 21, 2011, BPA, as a Transmission Operator, submitted a Self-Report citing noncompliance with MOD-029-1a R2, sub part R2.6. BPA reported that it was party to a contract with Portland General Electric (PGE) whereby BPA and PGE agreed to exchange the use of 100 MW of BPA's DC Intertie capacity, for 100 MW of PGE's AC intertie capacity. Although that contract was set to expire on July 1, 2012, BPA's posting of Total Transfer Capabilities (TTCs) for the AC and DC interties did not contemplate the termination of the contract on that date. Consequently, BPA posted TTCs that assumed the contract would extend through the NERC Available Transfer Capability (ATC) time horizon (from the next hour out to 13 months), beyond July 1, 2012. WECC reviewed BPA's Self-Report. WECC determined that BPA failed to allocate TTC on the ATC path per the terms of its contract with PGE. The contract expired on July 1, 2012. BPA, however, posted TTC calculations that assumed that the terms of the contract extended beyond July 1, 2012. Consequently, BPA TTC posts were not in accordance with the contractual agreement between BPA and PGE in noncompliance with R2.6. WECC, therefore, determined that BPA had an issue of MOD-029-1a R2.6 between April 1, 2011 through November 15, 2011, the date by which BPA completed its MOD-029-1a R2.6 Mitigation Plan.	WECC determined that this issue posed a minimal and not serious or substantial risk to the bulk power system. The risk posed by BPA noncompliance was limited. The overall sum of the TTCs for both the AC and DC Interties were not affected. The 100 MW decrease in the TTC for the AC intertie was offset by the 100 MW increase in the TTC for the DC intertie.	WECC has verified that BPA completed the following actions to mitigate this issue. BPA submitted a Mitigation Plan addressing noncompliance with MOD-029-1a R2.6. In that Mitigation Plan, BPA outlined the following actions: 1) BPA updated the AC and DC TTC allocation postings to reflect BPA's available DC TTC increased by 100 MW based on termination of the AC/DC Exchange Agreement. 2) BPA updated the AC and DC TTC allocation postings to reflect BPA's available AC TTC will be decreased by 100 MW based on the termination of the AC/DC Exchange Agreement.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Puget Sound Energy (PSE)	NCR05344	WECC201102625	IRO-STD-006-0	WR1	Pursuant to IRO-STD-006-0 WR1, a Load-Serving Entity shall comply with requests from Qualified Transfer Path Operators to take actions that will reduce Unscheduled Flow (USF) on the Qualified Path in accordance with the table titled "WECC Unscheduled Flow Procedure Summary of Curtailment Actions." On January 19, 2011, PSE submitted a Self-Report addressing an occurrence on October 16, 2010. Specifically, a USF event was determined at 13:06 PPT impacting Path 22-Southwest of Four Corners and escalated to a Step 4 Level 1 Curtailment event at 14:19 effective from 15:00 to 16:00 PPT. PSE initiated an interchange transaction for 15 MW commencing at 15:00 PPT. This transaction had a Transmission Distribution Factor on Path 22 of 13% in the qualified direction which represented a Restricted Transaction as defined by the Standard. This transaction established an obligation for PSE to provide relief of 1.9 MW on the qualified path through curtailment of the restricted transaction or some alternate action which would provide equivalent relief. PSE failed to curtail the restricted transaction or take any alternate action to provide equivalent relief on Path 22 during Step 4 of the USF event.	WECC determined this issue posed minimal risk to the reliability of the bulk power system (BPS) because this event involved one minor transaction, lasting one hour, encompassing only 1.9 MW of flow on a path rated 2,325 MW. The existence of the event was discovered by PSE performing a detailed study of circumstances after the fact. The study also determined that during the event, the Transmission Operator continued to have the option of curtailing transactions that were directly scheduled on the Qualified Path to reduce loading in the event of an overload. For these reasons, WECC determined this issue posed minimal risk to the reliability of the BPS.	PSE (1) revised its Operating Manual to remove any ambiguities with respect to restricted transactions; (2) PSE trained the appropriate personnel on USF events and updated USF training materials; and (3) PSE installed webSAS access on all RealTime Traders network computers to increase the visibility and utilization of the webSAS tool. WECC verified that the entity completed all mitigation activities.
Western Electricity Coordinating Council (WECC)	Puget Sound Energy (PSE)	NCR05344	WECC2011009044	TOP-003-1	R3	On December 29, 2011, PSE, as a Transmission Operator, Balancing Authority and Generator Operator, submitted a Self-Report to WECC for TOP-003-1 R3. PSE planned an AC power test in its Eastside Operations Energy Management System (EMS) data center on November 30, 2011, with the expectation of a temporary loss of its Inter-Control Center Protocol (ICCP). According to PSE, the testing was expected to result in four ICCP outages, each of less than five minutes, during four 15-minute outage windows. The first outage occurred from 10:15 to 10:18 but the entity failed to coordinate the outages and notified the Reliability Coordinator (RC) of the scheduled outages at 10:23 via phone call. Furthermore, it did not coordinate with other affected areas and notified the other affected areas via WECCNet at 10:27.	PSE initially failed to coordinate scheduled outages of communication channels (associated with its telemetering and control equipment) between the affected areas. However, from the time it started the first scheduled outage on its ICCP and until it informed its RC of the scheduled outage, only eight minutes had lapsed. At that time, the RC gave PSE permission to continue with its scheduled outages. An additional four minutes lapsed and PSE notified other affected areas of the scheduled outages using WECCNet. Once PSE notified the RC, the RC gave PSE permission to continue with the scheduled outages; PSE scheduled its outage in four fifteen-minute windows rather than a single extended outage; each scheduled outage lasted less than five minutes. For these reasons, WECC determined this issue posed minimal risk to the reliability of the bulk power system.	As previously described, PSE notified the RC and distributed applicable information to other areas using WECCNet, thus immediately remediating the issue. PSE also documented the roles and responsibilities associated with notifying affected areas for scheduled outages of telemetering and control equipment and associated communication channels; developed a checklist of required reliability and compliance tasks, including notification, for scheduled outages of telemetering and control equipment and associated communication channels to ensure notification to affected areas; and, trained applicable personnel to the documented roles and responsibilities and checklist.

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)	NCRXXXXX	FRCC2011007636	CIP-002-2	R3	FRCC_URE1 self-reported an issue with CIP-002-1 R3. Specifically, three Cyber Assets that were incorrectly identified as Critical Cyber Assets (CCAs) did not reside in the Electronic Security Perimeter (ESP). Additionally, one CCA was well-secured within the ESP but was not listed on the CCA list, resulting in an issue with CIP-002-3 R3. This issue existed for approximately thirteen months, until the CCA list was corrected.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because FRCC_URE1 only failed to document the list accurately and the CCA which was left off of the CCA list was within the secured ESPs and afforded the protections required for CCAs under the NERC CIP Standards. FRCC_URE1 also included three corporate workstations on the CCA list that were neither CCAs nor resided in the ESP. The error was documentary in nature and did not cause significant risk to BPS reliability because these Cyber Assets had no applications	To mitigate this issue, FRCC_URE1 updated its risk-based assessment methodology (RBAM) to re-evaluate and reapply risk-based criteria based on recently approved NERC Critical Asset selection criteria. FRCC_URE1 also updated and corrected its list of associated CCAs.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2) Pinellas County Resource Recovery (PCR)	NCRXXXXX	FRCC2012010599	CIP-002-1	R4	During a FRCC CIP Compliance Audit, it was determined that FRCC_URE2 did not maintain a null list of Critical Cyber Assets (CCAs) and did not obtain the required signature of the senior manager, resulting in an issue with CIP-002-1 R4. Specifically, beginning on the mandatory and enforceable date of the Standard, FRCC_URE2's risk-based assessment methodology (RBAM) included a documented Critical Asset (CA) null list and this document contained the senior manager's typed name, but not the ink signature. This version of FRCC_URE2's RBAM also did not contain a null list of CCAs, as required by the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because FRCC_URE2 documented the null list with no CAs but failed to document the null list with no CCAs. With respect to the signature requirement, a typed name was in the signature block, but was not an ink signature until the RBAM was revised. This issue resulted from lack of documentation, as FRCC_URE2 has no CAs or CCAs.	To mitigate this issue, FRCC_URE2 created the CCA null list and obtained the senior manager's signed and dated approval. Additionally, FRCC_URE2 scheduled the review of the future application of its RBAM and its results.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012010126	CIP-007-3	R5; R5.3.3	MRO_URE1 self-reported an issue with CIP-007-3 R5.3.3 for failing to ensure that Critical Cyber Asset (CCA) passwords were changed at least annually. MRO_URE1 uses a custom script to report the status of account passwords (expired, locked, or OK). The script incorrectly reported the status of two CCA user accounts as being "locked," when in fact they were not. The CCAs had an operating system automatic lock by means of password expiration. However two accounts did not have this expiration enabled and therefore were still accessible without an annual password change.	MRO 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. Although the two affected shared accounts did not have their passwords changed in the calendar year, both of the accounts had limited privileges and neither account had administrative privileges. The accounts are only used to launch the energy management system console applications, which require additional application-specific login credentials. Additionally, the account passwords were unchanged for less than two months (54 days) after expiration of the "annual" (once per calendar year) window.	MRO_URE1 performed a manual review of the database. The two user accounts were updated. The coding error within the custom script was identified and corrected. MRO verified that MRO_URE1 completed its mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011008450	CIP-006-3a	R2.2	NPCC_URE1 self-reported an issue with CIP-006-3a R2.2. NPCC_URE1 has a management services agreement pursuant to which a third party company serves as agent for NPCC_URE1 to perform reliability compliance functions and monitoring associated with NPCC_URE1's responsibilities as a NERC Registered Entity. During a NPCC CIP Compliance Audit of the third party's affiliate, it was determined that the third party, on behalf of NPCC_URE1, failed to timely perform a cyber vulnerability assessment for the servers that are involved with the physical access control system (PACS), as specified in CIP-007-3 R8. All other required assessments for NPCC_URE1's assets were completed, but a cyber vulnerability assessment had never been performed on the servers by the second quarter of 2010 as required by the Standard. The cyber vulnerability assessment was performed six months later. The third party company's parent company performs vulnerability assessments on a corporate level. Failure to complete the vulnerability assessment, as described above, affected multiple registered entities, including NPCC_URE1.	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 servers at issue are not used to monitor or control BPS assets. They control the card-reader system that is utilized to control the Physical Security Perimeter's (PSP) physical access points. In addition to the card-reader system, NPCC_URE1 utilizes security guards and video cameras to monitor access to the PSP. NPCC_URE1 also has strict controls in place for providing physical access to Critical Cyber Assets.	To mitigate this issue, the third party company, acting as the agent for NPCC_URE1, completed the vulnerability assessment for the servers at issue and revised its compliance assessment process document.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2012010670	CIP-006-3a	R1; R1.7	NPCC_URE2 self-reported an issue with CIP-006-3a R1.7. Specifically, NPCC_URE2 failed to update the physical security plan within 30 calendar days of the completion of any physical security system redesign or reconfiguration. The physical security plan was updated 155 days past the 30-day requirement. The issue was discovered while performing the "extent of condition analysis milestone" for a Mitigation Plan associated with another NPCC_URE2 subsidiary.	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 issue was administrative in nature. NPCC_URE2 updated the physical security plan, as required by the Standard, but did not do so within the specified time frame. In addition, all physical access control devices that provide access control, monitoring, and logging at the designated Physical Security Perimeters (PSPs) were functioning and operating properly.	To mitigate this issue, NPCC_URE2 updated its physical security plan to include that the physical security plan will be signed by the appropriate delegate for CIP-006. NPCC_URE2 also updated its corporate security workflow documentation for CIP-006 R1.7 to include a notification to the appropriate employee, as a checkpoint, when a physical security configuration change ticket is closed out for any physical security reconfiguration or redesign of PSPs at designated Critical Assets. NPCC_URE2 conducted an extent of condition analysis of PSPs at designated Critical Assets to determine whether there are other instances in which the physical security plan was not updated within 30 days following a reconfiguration or redesign change. NPCC_URE2 did not identify any additional issues in this analysis. NPCC_URE2 has communicated via email and conducted training with the applicable business areas regarding the changes to the enterprise physical security plan implemented by this Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2012009848	CIP-004-3	R4	RFC_URE1 self-reported an issue with CIP-004-3 R4 to Reliability*First*. A RFC_URE1 employee transferred from a position that required authorized cyber and authorized unescorted physical access to Critical Cyber Assets (CCAs) to a position that did not require such access. RFC_URE1's access revocation process is initiated by a Human Resource notification generated when RFC_URE1 updates an employee's personnel record to reflect a transfer. RFC_URE1 had revoked the employee's authorized cyber access. Due to the employee's transfer occurring on a holiday; RFC_URE1 did not update the personnel record that would initiate the access revocation process until three days after RFC_URE1 was required to revoke physical access. Upon discovery of the failure to revoke authorized unescorted physical access RFC_URE1 revoked such access.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. The RFC_URE1 employee transferred to a new position within the company and was still subject to its parent company's Code of Conduct and Corporate Policy for Cyber Security. Furthermore, prior to the time period of the issue, the employee had a valid personnel risk assessment as well as cybersecurity training. Finally, the employee did not physically access the CCAs during the time period of the issue, and RFC_URE1 timely revoked the employee's authorized cyber access.	RFC_URE1 provided refresher training to all human resource consultants responsible for initiating transfer employee access revocation and established an electronic reporting mechanism, which will reduce the manual intervention by multiple individuals and therefore reduce the risk of a repeat occurrence.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012001320	CIP-004-3	R4	RFC_URE2 self-reported an issue with CIP-004-3 R4 to Reliability*First*. The day after an employee resigned, RFC_URE2 revoked this employee's authorized cyber and authorized unescorted physical access to Critical Cyber Assets (CCAs), within the seven calendar days required. However, RFC_URE2 failed to update its authorized access list for several CCAs to reflect that this employee no longer had cyber access to CCAs. Eight days later, RFC_URE2 removed this employee from the authorized access list, as required by R4.1.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. RFC_URE2 timely revoked the employee's authorized cyber and authorized unescorted physical access to all CCAs. Thus, the employee had no ability to gain access to CCAs. In addition, the employee was not terminated for cause.	RFC_URE2 removed the employee from the authorized access list. In addition, RFC_URE2 counseled the individual's supervisor on the responsibilities for tickets submitted to process employee retirement, resignation, termination and displacement. Furthermore, RFC_URE2 enhanced its security request system to improve the timing and visibility of access removal requests. RFC_URE2 then communicated all improvements to the affected supervisors.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2012009854	CIP-004-3	R4	RFC_URE3 self-reported an issue with CIP-004-3 R4 to Reliability*First*. RFC_URE3 initially verbally self-reported this issue but seven days later memorialized this Self-Report in a Self-Report Form. The day after an employee retired, RFC_URE3 revoked this employee's authorized cyber and authorized unescorted physical access to Critical Cyber Assets (CCAs), within the seven calendar days required. However, RFC_URE3 failed to update its shared account authorized access list for one CCA to reflect that this employee no longer had access to the CCA. The CCA at issue is used for plant operation twenty-four hours a day and is typically logged on at all times to facilitate plant operation. RFC_URE3 discovered this issue during the quarterly verification of the authorized access list and removed this employee from the list approximately six weeks after his retirement date, as required by R4.1.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. RFC_URE3 timely revoked the employee's authorized cyber and authorized unescorted physical access to all CCAs, including the one at issue. In addition, RFC_URE3 timely changed the password to the shared account for the CCAs at issue. Thus, the employee had no ability to gain access to the CCA. In addition, the employee retired and was not terminated for cause. Furthermore, the CCA at issue is typically logged on at all times to facilitate plant operation. Therefore, it was less likely that the employee's name remaining on the access list would have caused unauthorized logons to the CCAs.	RFC_URE3 removed the employee from the authorized access list. In addition, RFC_URE3 updated the existing email distribution list in use for automatic notification of applicable employment status changes to include appropriate generation technical services compliance personnel. This revision will ensure that such individuals receive notice of employment status changes which will enable them to ensure the required updating of the authorized access lists.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC2012010023	CIP-007-3	R5	RFC_URE4 self-reported an issue with CIP-007-3 R5.3 to Reliability*First*. RFC_URE4 discovered that it did not change the passwords on 2 server accounts and 46 database accounts at least annually. RFC_URE4 determined that it incorrectly classified the servers as user accounts in its password database and missed the servers in its annual change activity. RFC_URE4 determined it failed to implement the procedure it has in place to initiate password changes for the 46 database accounts.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. Neither the 2 server accounts nor the 46 database accounts are related to assets supporting real-time control or monitoring functions. Additionally, both systems associated with the passwords at issue exist within an Electronic Security Perimeter (ESP) which requires separate active directory user accounts to gain access. Additionally, the directory user accounts necessary to gain access to the ESP expire on a 45-day cycle, resulting in multiple password changes to the directory user accounts during the duration of the issue.	In its Self-Report, RFC_URE4 stated that it had already changed, disabled and/or removed the passwords at issue. Additionally, RFC_URE4 revised its internal procedure to conduct password changes every six months, thereby decreasing the likelihood of exceeding the annual timeframe required by CIP-007-3 R5.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC2012009858	CIP-006-3c	R1.6.2	RFC_URE5 self-reported an issue with CIP-006-3c R1.6 to Reliability*First*. RFC_URE5 did have a visitor control program for visitors and a log to document the entry and exit of visitors, as required by R1.6; however, RFC_URE5 discovered that four individuals, three contractors and one employee (Employee), were not continuously escorted while inside a Physical Security Perimeter (PSP) for approximately 30 minutes on a single day. The Employee continuously escorted the three contractors; however, the Employee did not have authorized unescorted access to the PSP at issue. Reliability*First* determined the issue with CIP-006-3c R1 did not evidence an issue of CIP-004-3. CIP-004-3 sets forth personnel and training requirements for individuals with access to Critical Cyber Assets (CCAs). RFC_URE5's issue with CIP-006-3c R1 involved only Cyber Assets, not CCAs.	Reliability*First* determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the following factors. At the time of the issue, the PSP at issue was in the process of being decommissioned and did not enclose an Electronic Security Perimeter (ESP) or any active Cyber Assets. The PSP at issue contained Cyber Assets that had been removed from an ESP and were in storage until RFC_URE5 completed the disposal process. Also, prior to the Employee escorting the three contractors within the PSP, the Employee completed CIP training and RFC_URE5 performed a personnel risk assessment that revealed no issues that would preclude RFC_URE5 from granting the Employee access to the PSP at issue. The Employee qualified for authorized access to the PSP and, prior to the issue, RFC_URE5 properly granted the Employee unescorted physical access to other nearby PSPs. Furthermore, RFC_URE5 has a physical security plan and visitor control program that requires escorted access of visitors. This was an isolated incident in which the Employee and Employee's supervisor mistakenly believed the Employee was authorized to serve as an escort in the PSP at issue because the Employee was authorized to serve as an escort in surrounding PSP. RFC_URE5 conducted training, prior to and during the duration of the issue, on appropriate visitor control to help ensure compliance with CIP-006-3c R1.6.	RFC_URE5 subsequently granted the Employee access to the PSP at issue shortly after the issue. RFC_URE5 also provided the Employee with refresher training and feedback regarding RFC_URE5's visitor control program.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) Town of Waynesville (Waynesville)	NCRXXXXX	SERC2012010122	CIP-002-1	R1	During an audit, SERC determined that SERC_URE1 failed to provide evidence of procedures and evaluation criteria for its risk-based assessment methodology (RBAM) that was in place at the beginning of the compliance period in accordance with CIP-002-1 R1. SERC requested and reviewed additional information from SERC_URE1 in order to complete its assessment. SERC_URE1's initial RBAM consisted of printed copies of Standard CIP-002-1 with handwritten notes indicating that SERC_URE1 did not own assets listed in each of the R1.2 sub-requirements, and handwritten dates indicating review of the printed copy of CIP-002-1 and the hand-written notes. Based on this assessment, SERC_URE1 identified no Critical Assets. SERC staff determined that this document did not meet the requirements of CIP-002 R1. SERC_URE1 developed a RBAM that meets the requirements of CIP-002-3 R1.	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 because: 1. SERC_URE1 conducted an assessment to determine Critical Assets each year, even though it did not include evaluation criteria as required by the Standard; and 2. 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.	SERC verified that SERC_URE1 completed the following actions: SERC_URE1 implemented a RBAM that meets the requirements of CIP-002-3 R1.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC200900345	CIP-004-1	R4	The SERC spot check team reported an issue with CIP-004-1 R4, stating that SERC_URE2 could not provide evidence that it maintained lists of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) going back to when it was required to comply with the Standard. SERC_URE2 provided SERC with quarterly reviews of personnel with authorized cyber or authorized unescorted physical access to CCAs for the second, third, and fourth quarters of the year it was required to comply with the Standard. These quarterly reviews demonstrated that SERC_URE2 did not update its access lists in a timely manner and missed 30.93% of the total personnel. SERC_URE2 stated that the 30.93% of the individuals missing from the lists were authorized and had completed Personal Risk Assessments (PRA) and CIP cyber security training. SERC_URE2 provided evidence that PRAs had been conducted for sampled personnel and provided CIP cyber security training records for sampled personnel. Additionally, SERC_URE2 provided evidence showing that the missing individuals were accounted for and on a managed access list for the applicable individuals.	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: SERC_URE2 had authorized cyber or unescorted physical access to the 30 missing personnel and they had valid PRAs and CIP cyber security training.	SERC verified that SERC_URE2 completed the following actions: 1. Established a new written procedure that describes how the quarterly review of the list for access to Critical Cyber Assets located at a Control Center is to be conducted; 2. Under the new written procedure, the quarterly review of the list of personnel who have access to Critical Cyber Assets will take place within 14 calendar days after the last day of the quarter; 3. As part of its quarterly review, SERC_URE2 will compare the list of those who actually have access (the print out form the server controlling the control center card access system) against the working list (a paper document kept at the control center security desk); 4. If no discrepancies are identified from this comparison, the print out from the server controlling the control center card access system will become the new working list for purposes of the next quarter; 5. If a discrepancy is identified, the discrepancy will be resolved to assure that physical access is granted only to those employees who need daily access to the control center and who have completed the required personnel risk assessment and training. The new working list for purposes of the next quarter will reflect the resolution of these discrepancies; and
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3) Greenwood Utilities Commission (Greenwood)	NCRXXXXX	SERC2011008613	CIP-002-1	R1	During an audit, SERC determined that SERC_URE3 had failed to develop a sufficient risk-based assessment methodology (RBAM) for determining whether or not it had Critical Assets that included all of the requirements in accordance with CIP-002-1 R1. The documentation provided by SERC_URE3 to demonstrate its compliance with CIP-002-1 R1 failed to describe a RBAM that included procedures and evaluation criteria for identifying Critical Assets and failed to address the assets in R1.2.1 through R1.2.7 and how SERC_URE3 would evaluate whether any such assets should be considered Critical Assets in the event SERC_URE3 acquired them.	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. SERC_URE3 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.	SERC staff verified that SERC_URE3 completed the following actions: SERC_URE3 developed a RBAM that includes procedures and evaluation criteria for identifying Critical Assets and addresses all the assets identified in CIP-002-1 R1.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3) Greenwood Utilities Commission (Greenwood)	NCRXXXXX	SERC2011008614	CIP-003-1	R2	During an audit, SERC determined that SERC_URE3 failed to provide evidence assigning a senior manager with overall responsibility for leading and managing SERC_URE3's implementation of, and adherence to, Standards CIP-002-1 to CIP-009-1 in accordance with CIP-003-1 R2 for approximately three years. SERC_URE3 provided documentation demonstrating that it had authorized the signing of documents on behalf of SERC_URE3 by senior vice-presidents for SERC and NERC matters and identified a single point of contact for the SERC_URE3 internal compliance program, but the documentation did not demonstrate that SERC_URE3 had assigned a senior manager responsible for leading and managing SERC_URE3's implementation of, and adherence to, Standards CIP-002 through CIP-009 for approximately three years.	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. SERC_URE3 had identified a senior manager as its single point of contact for the SERC_URE3 utilities program. This single point of contact was responsible for approving the risk-based methodology, list of Critical Assets, and list of Critical Cyber Assets; and 2. SERC_URE3 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.	SERC verified that SERC_URE3 completed the following actions: SERC_URE3 assigned a senior manager with overall responsibility for leading and managing SERC_URE3's implementation of, and adherence to, Standards CIP-002 to CIP-009.

Document Accession #: 20120831-5290 Filed Date: 08/31/2012

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 3 (SERC_URE3) Greenwood Utilities Commission (Greenwood)	NCRXXXXX	SERC2012010547	CIP-002-1	R4	SERC_URE3 self-reported an issue with CIP-002-1 R4, stating that a SERC_URE3 employee approved the risk-based assessment methodology (RBAM), the null list of Critical Assets, and the null list of Critical Cyber Assets prior to being designated as the senior manager with overall responsibility for leading and managing SERC_URE3's implementation of, and adherence to, Standards CIP-002 through CIP-009. This Self-Report was submitted in response to an inquiry from SERC staff during an assessment of a separate enforcement action. SERC determined that SERC_URE3 did not formally assign a senior manager with overall responsibility for leading and managing SERC_URE3's implementation of, and adherence to, CIP-002 through CIP-009 for approximately three years. Accordingly, all of SERC_URE3's approvals of its RBAM, Critical Asset list, and Critical Cyber Asset list prior to the designation of a senior manager were not in compliance with the relevant Reliability Standards.	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. SERC_URE3 had identified a senior manager as its single point of contact for the SERC_URE3 utilities program. This single point of contact was responsible for approving the risk-based methodology, list of Critical Assets, and list of Critical Cyber Assets; and 2. SERC_URE3 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.	SERC verified that SERC_URE3 completed the following actions: SERC_URE3's newly appointed senior manager with overall responsibility for leading and managing SERC_URE3's implementation of, and adherence to, Standards CIP-002 through CIP-009 signed and approved SERC_URE3's RBAM, Critical Asset list, and Critical Cyber Asset list.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2012010138	CIP-002-3	R2	During an audit, SERC determined that SERC_URE4 failed to provide evidence of a Critical Asset list determined through its annual application of the risk-based assessment methodology (RBAM) in accordance with CIP-002-3 R2. SERC reviewed documents provided by SERC_URE4 and determined that SERC_URE4 had RBAMs from three prior years. The three prior years' RBAMs stated that SERC_URE4 had no Critical Assets and no Critical Cyber Assets (CCAs). SERC staff determined that SERC_URE4 could not provide evidence it developed its list of Critical Assets in a prior year.	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 because: 1. SERC_URE4 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_URE4 applied three prior years' RBAMs, resulting in null lists for Critical Assets, indicating that SERC_URE4 did not acquire any Critical Assets in the missing year.	SERC verified that SERC_URE4 completed the following actions: 1. Completed the annual review and approval of its RBAM, including the approval of null lists for Critical Assets and CCAs; and 2. Added review dates for the annual review of its RBAM, Critical Assets, and CCAs and required approvals to calendar reminders for the responsible parties.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2012010139	CIP-002-3	R3	During an audit, SERC determined that SERC_URE4 failed to provide evidence of an associated list of Critical Cyber Assets (CCAs) derived from its list of Critical Assets in a prior year in accordance with CIP-002-3 R3. SERC reviewed documents provided by SERC_URE4 and determined that SERC_URE4 had risk-based assessment methodologies (RBAMs) from three prior years. The three prior years' RBAMs stated that SERC_URE4 had no Critical Assets and no CCAs. SERC staff determined that SERC_URE4 could not provide evidence that it had developed a list of CCAs in a prior year.	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 because: 1. SERC_URE4 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_URE4 applied three prior years' RBAMs, resulting in null lists for Critical Assets and CCAs, indicating that SERC_URE4 did not acquire any Critical Assets or CCAs in the missing year.	SERC verified that SERC_URE4 completed the following actions: 1. Completed the annual review and approval of its RBAM, including the approval of null lists for Critical Assets and CCAs; and 2. Added review dates for the annual review of its RBAM, Critical Assets, and CCAs and required approvals to calendar reminders for the responsible parties.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2012010140	CIP-002-2	R4	During an audit, SERC determined that SERC_URE4 failed to present a signed and dated record of the Senior Manager or delegate's approval of the risk-based assessment methodology (RBAM), the list of Critical Assets, and the list of Critical Cyber Assets (CCAs) for a calendar year in accordance with CIP-002-2 R4. SERC reviewed documents provided by SERC_URE4 and determined that SERC_URE4 failed to approve the RBAM, the list of Critical Assets, and the list of CCAs for one year. SERC staff determined that SERC_URE4 personnel signed the null list of Critical Assets and the null list of CCAs in three prior years. Despite this fact, the individuals signing these lists in two prior years were not valid signers because they had not been assigned responsibility in writing for SERC_URE4's compliance with the CIP standards as required by CIP-003 R2. Therefore, SERC_URE4's issue with CIP-002 R4 extended back to when SERC_URE4 was required to be compliant with the Standard. Also, the RBAM was not approved in two prior years as required by versions 2 and 3 of the Standard.	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 because: 1. SERC_URE4 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_URE4 applied three prior years' RBAMs, resulting in null lists for Critical Assets and CCAs, indicating that SERC_URE4 did not acquire any Critical Assets or CCAs in the missing year.	SERC verified that SERC_URE4 completed the following actions: 1. Completed the annual review and approval of its RBAM, including the approval of null lists for Critical Assets and CCAs; 2. Added review dates for the annual review of its RBAM, Critical Assets, and CCAs and required approvals to calendar reminders for the responsible parties; and 3. Reformatted the RBAM signoff to incorporate an approval signature.

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 4 (SERC_URE4)	NCRXXXXX	SERC2012010141	CIP-003-2	R2	During an audit, SERC determined that SERC_URE4 failed to provide evidence showing that the designated senior manager was assigned the role at the beginning of the compliance period in accordance with CIP-003-2 R2. SERC reviewed documents provided by SERC_URE4 and determined that SERC_URE4 did not properly assign a Senior Manager with overall responsibility and authority for leading and managing SERC_URE4's implementation of, and adherence to the CIP Standards. However, because SERC_URE4 identified that it had no Critical Cyber Assets in a prior year it was exempt from compliance with CIP-003-1 R2, and was only required to be compliant when CIP-003-2 R2 became effective.	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 because: 1. SERC_URE4 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_URE4 applied three prior years' RBAMs, resulting in null lists for Critical Assets and CCAs, indicating that SERC_URE4 did not acquire any Critical Assets or CCAs in the missing year.	SERC verified that SERC_URE4 completed the following actions: Created a document that properly defines the single CIP Senior Manager by title, name, and date of designation.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 5 (SERC_URE5) LSP Energy Limited Partnership (LSP)	NCRXXXXX	SERC2012010638	CIP-003-3	R2	SERC_URE5 self-reported an issue with CIP-003-3 R2, stating that SERC_URE5 did not designate a new senior manager within 30 days of the departure of SERC_URE5's previous senior manager. SERC requested and reviewed documentation of SERC_URE5's designation of the senior manager. SERC_URE5 provided documentation showing that a senior manager was designated and documented, but the senior manager left unexpectedly approximately seven months later. SERC_URE5 failed to formally assign a new senior manager until 193 days later, but did have a plant manager acting as the CIP senior manager during this period. SERC_URE5 also provided a document detailing its leadership designation program, which requires the identification of the senior manager, delegates, and any changes to the senior manager be documented within 30 calendar days of the effective date. SERC_URE5's leadership designation program stated that there were no exceptions identified for its cyber security policy. SERC_URE5 also confirmed that it had not assigned any delegates. SERC found that SERC_URE5 had a documented program in place that met the intent of the Requirement but that SERC_URE5 had failed to comply	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 because: 1. SERC_URE5 had a plant manager acting as the CIP senior manager during the period in question even though he was not officially delegated; and 2. SERC_URE5 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.	SERC verified that SERC_URE5 completed the following actions: 1. SERC_URE5 designated a new senior manager; and 2. SERC_URE5 placed a transfer note with instructions in the plant manager's personnel file stating that he is the senior manager with responsibility for the CIP standards and instructing the plant manager to properly transfer the senior manager duties to an appropriate plant staff member upon transfer, retirement, or other long-term change in status with the facility.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 5 (SERC_URE5) LSP Energy Limited Partnership (LSP)	NCRXXXXX	SERC2012010676	CIP-002-1	R4	SERC_URE5 self-reported an issue with CIP-002-1 R4, stating that SERC_URE5 failed to have a senior manager or delegate(s) annually approve the list of Critical Assets and Critical Cyber Assets (CCAs) in two prior years. SERC requested and reviewed additional information in order to complete its assessment. SERC found that SERC_URE5 applied its established risk-based assessment methodology (RBAM) to all associated assets, resulting in null lists for Critical Assets and CCAs. SERC_URE5's senior manager failed to sign and date the Critical Asset and CCA list for two prior years. SERC_URE5's senior manager signed the RBAM for four consecutive years. SERC_URE5's senior manager approved and signed the Critical Asset and CCA lists, which were null, for two prior years.	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 because: 1. SERC_URE5's senior manager approved and signed the RBAM; and 2. SERC_URE5 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.	SERC verified that SERC_URE5 completed the following actions: 1. Hired a third party to replace SERC_URE5's existing compliance program with a new reliability compliance program; 2. Used the new reliability compliance program to determine and document if SERC_URE5 had any Critical Assets or CCAs; 3. Had the senior manager sign the RBAM, Critical Asset list, and CCA list for two prior years; and 4. Filed documentation appropriately at the facility as evidence of compliance.

Document Accession #: 20120831-5290 Filed Date: 08/31/2012

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPPRE_URE1)	NCRXXXXX	SPP201000247	CIP-004-1	R3	During a Multi-Region Spot Check, SPP RE determined that SPPRE_URE1 had an issue with CIP-004-1 R3 for a failure to perform personnel risk assessments (PRAs) to all personnel with unescorted physical access to Critical Cyber Assets (CCAs). The Spot Check team sampled PRA records of individuals having authorized cyber or authorized unescorted physical access to SPPRE_URE1's CCAs. At the time of the Spot Check, SPPRE_URE1 had an agreement in place with Entity A, which co-owns and operates Substation A. SPPRE_URE1 owns the 115 kV assets located at Substation A, including certain assets that were, at the time of the Spot Check, deemed CCAs. The agreement provided that Entity A would perform PRAs on its employees that were granted authorized unescorted physical access to the CCAs at Substation A. SPPRE_URE1 requested and received quarterly confirmation via email that Entity A personnel with CCA access met the requirements of CIP-004-1, including the PRA requirement. One such Entity A employee was included in the group of PRA records sampled by the Spot Check team for CIP-004-1 R3 compliance. When SPPRE_URE1 requested PRA documentation from Entity A for that employee, Entity A informed SPPRE_URE1 that the PRAs had not been performed for the fifteen Entity A employees with authorized unescorted physical access to Substation A and that the quarterly emails verifying compliance had been provided in error. As a result, SPPRE_URE1 did not comply with CIP-004-1 R3 because it did not ensure that PRAs were performed for all personnel with authorized unescorted physical access to CCAs.	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 Entity A did not perform PRAs on its employees who were granted access to the Entity A / SPPRE_URE1 substation that housed SPPRE_URE1's CCAs, the access that the Entity A employees had was physical only. The Entity A employees did not have electronic access to the CCAs – the devices were only accessible by dial-up and used non-routable protocols. According to a NERC CIP-006-1 interpretation, because there is minimal risk of compromising other CCAs, dial-up devices that use non-routable protocols, such as the ones at issue, are not required to be enclosed within a "six-wall" physical border. Because no "six-wall" physical border is required for these devices, unescorted physical access to the devices presents a minimal risk. Therefore, SPP RE determined that the unescorted physical access to the SPPRE_URE1's devices at issue presented a minimal risk to the reliability of the BPS.	When SPPRE_URE1 determined that Entity A had not complied with its agreement with SPPRE_URE1, immediate action was taken to remove physical access for all Entity A employees pending implementation of other measures. That physical access was removed shortly after the issue was identified during the Spot Check and before the day was over. Subsequently, SPPRE_URE1 removed the modem and the dial-up telephone line connection to the CCAs; therefore, the devices at the substation in question were no longer CCAs. SPPRE_URE1 subsequently updated the status of these devices on the CCA list to non-critical. A new agreement was executed between SPPRE_URE1 and Entity A specifying that the parent company for SPPRE_URE1 will perform PRA's for Entity A employees or contractors requiring access to CCAs in SPPRE_URE1 substations. SPP RE verified completion of these mitigating activities.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPPRE_URE2)	NCRXXXXX	SPP2012009412	CIP-005-3a	R2; R2.2	SPPRE_URE2 self-certified a noncompliance of CIP-005-3a R2.2 for a failure to enable only ports and services required for operations and for monitoring Cyber Assets (CAs) within the Electronic Security Perimeter (ESP). SPPRE_URE2 reported that two of its Unified Threat Management (UTM) devices, which acted as routers and as access points to an ESP, had ports open that were not specific to the operation and monitoring of CAs within the ESP.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The UTM devices were connecting a control center ESP with another control center ESP via a private microwave link owned and operated by SPPRE_URE2. The UTMs were not linked to the outside world and only connected the control center ESPs, thereby reducing the risk to minimal.	After discovery of the open ports on the two UTM network devices, SPPRE_URE2 reviewed documentation concerning the ports and services to the UTMs, made modifications to the configuration files, uploaded new configurations to the UTMs in the test environment, and ran the complete system for 48 hours to ensure the new configurations did not affect the test system and that the test system operated in a reliable manner. Once the 48-hour window of testing was complete, SPPRE_URE2 loaded the newly tested configuration to the live system UTMs. SPPRE_URE2 successfully uploaded the new configuration and the EMS/SCADA system operated in a reliable manner.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPPRE_URE3) Western Farmers Electric Cooperative (WFEC)	NCRXXXXX	SPP2012009923	CIP-003-3	R1; R1.1	During a SPP RE CIP Audit of SPPRE_URE3 the SPP RE Audit team discovered an issue with CIP-003-3 R1.1 for a failure to address all of the requirements in Standards CIP-002-3 through CIP-009-3 in its cyber security policy. Specifically, SPP RE found that SPPRE_URE3 failed to address one NERC requirement CIP-003-3 R4 (information protection associated with CCAs) in its cyber security policy, which is required by CIP-003-3 R1.1.	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). This instance of noncompliance presented a documentation issue. Prior versions of SPPRE_URE3's cyber security policy did include all requirements in NERC Standards CIP-002 through CIP-009; the latest revision, however, failed to include the one requirement. Furthermore, while SPPRE_URE3 failed to include CIP-003-3 R4 in its cyber security policy, SPPRE_URE3 did have an implemented and documented program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4.	SPPRE_URE3 amended its cyber security policy to include CIP-003-3 R4. SPP RE verified completion of the mitigation activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX CSGP Services, LP (CSGP)	TRE2012009949	CIP-002-1	R1	During an Audit, Texas RE determined that Texas RE_URE1's documented risk-based assessment methodology (RBAM) did not include its Qualified Scheduling Entity (QSE) control centers within the scope of assets to be considered for evaluation when identifying Critical Assets (CAs), which presented an issue with CIP-002-1 R1. Texas RE_URE1 has delegated some of its responsibilities to its QSE. As a result, the QSE control centers were not included in Texas RE_URE1's RBAM used to identify CAs. Texas RE determined that the start date of this issue was from when Texas RE_URE1 was required to comply with this Standard to when Texas RE_URE1 updated its RBAM and re-performed its CAs identification with consideration given to its QSE's control centers. The identification showed that Texas RE_URE1 had no CAs.	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 did not and does not own any CAs or Critical Cyber Assets (CCAs) at any time. The inclusion of the QSE in Texas RE_URE1 RBAM did not yield any new CAs or CCAs. Also, the QSE that was not considered does not have the ability to control the Texas RE_URE1 facility. Therefore, Texas RE determined that this issue was documentation related.	Texas RE_URE1 revised its procedures to include consideration of its QSE when performing its RBAM. Texas RE_URE1 has also re-performed its CAs identification and has determined that it does not own any CA or CCAs. Texas RE verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1) Pacific Gas and Electric Company (PGAE)	NCRXXXXX	WECC2012010360	CIP-006-2	R1	During an internal review of CIP-006 compliance, WECC_URE1 self-reported an issue with CIP-006-2 R1. WECC_URE1 failed to ensure its Physical Security Plan was reviewed and approved by the CIP senior manager or delegate. While WECC_URE1 did document, implement and maintain a Physical Security Plan approved by a senior manager, it failed to implement the approval required upon the effective date of CIP-006 Version 2. WECC reviewed WECC_URE1's Self-Report and determined the Physical Security Plan was not approved by "the" Senior Manger as required by CIP-006 R1 Versions 2 and 3. Although WECC_URE1's Physical Security Plan was approved by "a" senior manager, this was not "the" assigned Senior Manager or delegate at the time of the approval. WECC_URE1 stated that this was a result of failure to update the approval required for the Physical Security Plan upon the effective date of Version 2. Specifically, CIP-006 R1 changed from "The Responsible Entity shall create and maintain a physical security plan approved by a senior manager" in Version 1 to "The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager" in Version 2. Based on the Physical Security Plan documentation, WECC_URE1 did document, implement and maintain a plan, however it failed to recognize the implications of the change in wording of the CIP-006 Standard from Version 1 to Version 2. Once identified, WECC_URE1 delegated the individual responsible for approving the CIP-006 Plan per its CIP-003 R2 senior manager assignment. WECC determined that WECC_URE1 failed to implement CIP-006-2 R1.	WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because even though the Physical Security Plan was not maintained and approved by the assigned CIP Manager, it was maintained and approved by the individual who is responsible for WECC_URE1's overall corporate security. Additionally, after the noncompliance was discovered, WECC_URE1 assigned the individual as a delegate for the CIP Senior Manager. WECC determined that this was WECC_URE1's second occurrence of CIP-006 R1. Although this is WECC_URE1's second occurrence of CIP-006 R1, WECC determined that the issue addressed herein involves different conduct. Specifically, the CIP-006 violation addressed herein is distinct from the previous CIP-006 violation in that the first violation pertained to unescorted access, whereas the current CIP-006 issue was a result of WECC_URE1 failing to update the approval required for the Physical Security Plan upon the effective date of Version 2. For these reasons, WECC determined WECC_URE1's CIP-006 compliance history should not preclude the current CIP-006 issue from being an FFT. Therefore, WECC determined that FFT was appropriate for the current CIP-006 issue.	WECC_URE1's Physical Security Plan approval was completed. WECC_URE1 prepared a letter of delegation, signed by the assigned CIP Senior Manager to include a delegate for the CIP Senior Manager. Further, WECC_URE1 implemented an automated tracking tool to help track due dates of recurring requirements. WECC reviewed this evidence and verified WECC_URE1's completion of the Mitigation Plan.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2) Southern California Edison - Transmission & Distribution Business Unit (SCET)	NCRXXXXX	WECC2012009855	CIP-003-1	R1.3	WECC_URE2 self-certified noncompliance with CIP-003-1 R1.3 stating that it did not annually review its entire cyber security policy in 2009 and 2010. The policies that were not reviewed were outdated and not used by WECC_URE2 but, nevertheless, were a part of its cyber security policy. WECC_URE2 employees were aware not to follow the outdated policies. WECC determined that WECC_URE2 failed to perform a complete annual review of its cyber security policy for the calendar years 2009 and 2010.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because in this instance, while policies that are a part of the cyber security policy were not reviewed, those policies were outdated and not used by the entity. As compensating measures, WECC_URE2 performed annual reviews and approved the current policies in use.	WECC_URE2 reviewed its cyber security policy in calendar year 2011 and removed the outdated items.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) Southern California Edison - Generation - Power Production Business Unit (SCEG)	NCRXXXXX	WECC2012010762	CIP-003-1	R1.3	WECC_URE3, self-certified noncompliance with CIP-003-1 R1.3. According to WECC, WECC_URE3 stated that it did not annually review its entire cyber security policy in calendar year 2010. The policies that were not reviewed were outdated and not used by WECC_URE3 but, nevertheless, were a part of WECC_URE3's cyber security policy. WECC determined that WECC_URE3 failed to perform a complete annual review of its cyber security policy for the calendar year 2010.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because while policies that are a part of the policy were not reviewed, those policies were outdated and not used by the entity. As compensating measures, WECC_URE3 stated that it did annual reviews and approved the current policies in use.	WECC_URE3 reviewed its cyber security policy in calendar year 2011 and removed the outdated items.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4) San Carlos Irrigation Project (SCIP)	NCRXXXXX	WECC2012010696	CIP-002-1	R3	WECC performed an offsite compliance audit of WECC_URE4's compliance with, among other Reliability Standards, CIP-002-1 R3. The Audit Team concluded that WECC_URE4 had an issue of CIP-002-1 R3 because it failed to develop a null list of its Critical Cyber Assets (CCAs). The Audit Team also concluded that WECC_URE4 knew it did not have any CCAs because it had developed a null list of its Critical Assets. WECC has determined that WECC_URE4 had an issue of CIP-002-1 R3 because it failed to develop a null list of its CCAs. WECC further determined that the duration of the issue was from when the Standard became enforceable for WECC_URE4, until when it developed its null list of CCAs.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. WECC_URE4 had previously applied its risk-based assessment methodology and knew prior to the start of the issue that it did not have any Critical Assets and, therefore, did not have any CCAs. Thus, the potential for malicious conduct to CCAs did not exist.	WECC_URE4 developed a null list of its CCAs.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4) San Carlos Irrigation Project (SCIP)	NCRXXXXX	WECC2012010697	CIP-002-1	R4	WECC performed an offsite compliance audit of WECC_URE4's compliance with, among other Reliability Standards, CIP-002-1 R4. The Audit Team concluded that WECC_URE4 had an issue of CIP-002-1 R4 because it failed to have a CIP senior manager sign its null list of its Critical Cyber Assets CCAs. However, the Audit Team also concluded that WECC_URE4 knew it did not have any CCAs because it had developed a null list of its Critical Assets. WECC determined that WECC_URE4 had an issue of CIP-002-1 R4 because it failed to have a CIP senior manager sign its null list of Critical Assets and CCAs. WECC further determined that the duration of the issue was from when the Standard became enforceable for WECC_URE4, until when its CIP senior manager signed its null list of Critical Assets and CCAs.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. After applying its risk-based assessment methodology, WECC_URE4 knew it did not have any Critical Assets and therefore did not have any CCAs prior to the issue. Thus, the potential for malicious conduct to CCAs did not exist.	WECC_URE4's CIP senior manager signed its null list of its CCAs.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4) San Carlos Irrigation Project (SCIP)	NCRXXXXX	WECC2012010699	CIP-003-1	R2	WECC performed an offsite compliance audit of WECC_URE4's compliance with, among other Reliability Standards, CIP-003-1 R2. The Audit Team concluded that WECC_URE4 had an issue of CIP-003-1 R2 because it failed to designate a CIP senior manager with overall responsibility and authority for CIP-002 through CIP-009. The Audit Team also concluded that WECC_URE4 knew it did not have any Critical Cyber Assets because it had developed a null list of its Critical Assets. WECC determined that WECC_URE4 had an issue of CIP-003-1 R2 because it failed to designate a CIP senior manager with overall responsibility and authority for CIP-002 through CIP-009. WECC further determined that the duration of the issue was from when the Standard became enforceable for WECC_URE4, until when it designated a CIP senior manager with overall responsibility and authority for CIP-002 through CIP-009.	WECC determined that this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. After applying its risk-based assessment methodology, WECC_URE4 knew it did not have any Critical Assets and therefore did not have any CCAs prior to the issue. Thus, the potential for malicious conduct to CCAs did not exist.	WECC_URE4 designated a CIP senior manager with overall responsibility and authority for CIP-002 through CIP-009.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2012009653	CIP-003-3	R5	WECC_URE5 submitted a Self-Report citing facts consistent with an issue of CIP-003-1 R5.3. Specifically, WECC_URE5 reported two instances in which employees were granted access to Critical Cyber Asset (CCA) information without completing request training required under WECC_URE5's CCA program. The first instance occurred after an employee was granted electronic access to WECC_URE5's CIP document library (Library) without completing training per WECC_URE5's CIP program. The second instance of noncompliance occurred after an employee was granted access to the Library in error. WECC_URE5 detected the mistake and revoked this employee's access rights. Enforcement reviewed WECC_URE5's Self-Report and determined these two instances demonstrate that WECC_URE5 failed to manage access to CCA information in compliance with its CCA program.	WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The purpose of CIP-003 is to ensure that Responsible entities have minimum security management controls in place to protect CCAs. To that end, CIP-003-1 R5 requires entities to document and implement a program for managing access to protected CCA information. In this case, WECC_URE5 granted access to CCA information to two individuals who did not complete requisite training per WECC_URE5's CCA program. The risks, posed by WECC_URE5 noncompliance are, however, offset in that WECC_URE5 quickly detected and mitigated both instances of noncompliance within 23 days. Further, based on WECC_URE5's prompt detection and mitigation, there is evidence that demonstrates WECC_URE5 regularly reviews its access privilege lists throughout the year instead of waiting for an annual review. Risks are further mitigated given the limited scope of the issue. The first individual granted access had only to complete training, a requirement unique of WECC_URE5's program that is above and beyond the criteria prescribed under R5. In the second instance, although WECC_URE5 mistakenly granted access to the second individual, that individual never accessed or attempted to access CCA information during the 23 days prior to WECC_URE5's detection and revocation of that individual's access. Enforcement, therefore, determined that the risks posed by WECC_URE5 noncompliance posed a minimal risk to the bulk power system.	WECC_URE5 ensured that the first individual completed request training. WECC_URE5 revoked access for the second individual.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 6 (WECC_URE6)	NCRXXXXX	WECC2011009022	CIP-006-3a	R2.2	WECC_URE6 self-reported an issue of CIP-006-3 R2.2. A WECC subject matter expert (WECC SME) contacted WECC_URE6 to discuss its Self-Report. According to the WECC SME, WECC_URE6 stated that it did not afford two panels the protections of CIP-007 R6. The panels involved control access to all of WECC_URE6's Physical Security Perimeters (PSPs).	WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The panels are located in a PSP inside a locked cabinet with restricted key access to which fewer than five individuals have access. The locked cabinets also have tamper switches installed to alert the entity upon opening the enclosures. For these reasons, WECC determined these issues posed minimal risk to the reliability of the bulk power system.	WECC_URE6 stated that the panels are located in a PSP inside a locked cabinet with restricted key access to which few individuals have access. The locked cabinets also have tamper switches installed to alert the entity upon opening the enclosures. WECC_URE6 submitted a Technical Feasible Exception for the devices involved.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 7 (WECC_URE7)	NCRXXXXX	WECC2011008706	CIP-005-3a	R1	WECC_URE7 submitted a Self-Report to WECC for CIP-005-3a R1. WECC_URE7 decommissioned hard drives associated with firewall management consoles, which were Cyber Assets used in the access control and monitoring WECC_URE7's Electronic Security Perimeter. During the disposal and decommissioning process, WECC_URE7 did not provide the protective measure specified in CIP-007 R7.3 to the hard drives. Specifically, WECC_URE7 did not follow its CIP-007 R7 disposal and redeployment procedures, resulting in an issue with CIP-005-1 R1.	WECC determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. WECC_URE7 stored the hard drives in a locked cabinet in a secure facility that requires card key access. Further, only IT personnel had access to the area in which the hard drives resided. Additionally, the hard drives were part of a redundant array of independent disks (RAID) where no single disc would have been available for data retrieval without the other participating discs in that RAID array. For these reasons, WECC determined the issue posed minimal risk to the reliability of the bulk power system.	WECC_URE7 moved the hard drives into a Physical Security Perimeter upon discovering the issue. Further, WECC_URE7 took the following five steps to mitigate the root cause of the issue: 1) Added an additional requirement to the WECC_URE7 change management procedure requiring persons reviewing and approving changes to review all documentation. 2) Provided additional clarity in documented procedures on safeguarding of Cyber Assets during disposal and redeployment. 3) Developed refresher training specific to disposal and redeployment procedures which includes testing for comprehension and retention. 4) Ensured disposal and redeployment re-training is completed by all applicable WECC_URE7 employees. 5) Updated required annual NERC CIP Training to include a module specific to disposal and redeployment.

Document Accession #: 20120831-5290 Filed Date: 08/31/2012

Document Content(s)