Federal Energy Regulatory Commission
Washington, D.C. 20426
January 5, 2022

Re: FOIA No. FY19-30 (RC12-14)
Forty Sixth Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated December 14, 2021, the submitter and certain Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. RC12-14, along with the names of four (4) 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, I conclude that disclosure of these URE identities is appropriate and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC12-14.

---

[1] 5 U.S.C. § 552 (2018).

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

With respect to the remaining identities of UREs contained in RC12-14, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the following: the nature of the Critical Infrastructure Protection (CIP) violation, including whether there is a Technical Feasibility Exception involved that does not allow the Unidentified Registered Entity to fully meet the CIP requirements; whether vendor-related information is contained in the Notices of Penalty (NOP); whether mitigation is complete; the content of the public and non-public versions of the NOP; the extent to which the disclosure of the identity of the URE and other information would be useful to someone seeking to cause harm; whether a successful audit has occurred since the violation(s); whether the violation(s) was administrative or technical in nature; and the length of time that has elapsed since the filing of the public NOP. An application of these factors will dictate whether a particular FOIA exemption, including 7(F) and/or Exemption 3, is appropriate. *See Garcia v. U.S. DOJ,* 181 F. Supp. 2d 356, 378 (S.D.N.Y. 2002) ("In evaluating the validity of an agency's invocation of Exemption 7(F), the court should within limits, defer to the agency's assessment of danger.") (citation and internal quotations omitted).

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-14 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: 2022.01.05 10:13:18 -05'00'

Benjamin Williams
Deputy Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

RC12-14

July 31, 2012

CER-Colorado Bend Energy Partners LP (Colorado Bend) - .pdf page 28-29

CER-Quail Run Energy Partners LP (Quail Run) - .pdf page 29-30

Southern California Edison - Transmission & Distribution Business Unit (SCET) - .pdf page 31

Pacific Gas and Electric Company (PGAE) - .pdf page 31

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 30 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 46 possible violations[5] of 19 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 46 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 and Track Report Spreadsheet, included as Attachment A; and
b) Additions to the service list, included as Attachment B.

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

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

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

Attachment a

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

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR JULY 2012 FIND FIX AND TRACK 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*
Manager of Compliance Enforcement
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6887
(801) 883-6894 – facsimile
CLuras@wecc.biz

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
July 31, 2012

Take notice that on July 31, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty (30) 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)	JEA	NCR00040	FRCC2012010070	PER-003-0	R1	On April 16, 2012, JEA, as a Balancing Authority and Transmission Operator, self-reported that it had a system operator operating the Bulk Electric System (BES) who was late in paying the re-certification fee to NERC for her NERC Reliability Coordinator (RC) certification, resulting in RC certificate suspension and revocation. The employee was operating the BES from March 17, 2011 to April 3, 2012 without the required certification.	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 system operator had all of the training hours required to maintain her NERC RC certification and was an experienced system operator who had been NERC RC-certified since at least 2006.	JEA communicated with all system operators on the NERC certification renewal process, including the importance of the administrative components of the process. Further, JEA requested that all system operators allow the manager of bulk power operations access to their records. In addition, JEA developed and implemented a procedure under which JEA management is able to verify credentials with NERC at least 30 days prior to expiration, verify again at seven days, and remove the operator from shift rotation prior to the expiration date if documentation is not provided to verify updated certification. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Southern Power Company (SC)	NCR00071	FRCC2012009803	PRC-005-1a	R2	On February 24, 2012, SC, as a Generator Owner, self-reported that it identified two months, September and October 2011, where it could not demonstrate evidence of monthly battery testing on a temporary battery bank, as required by its generation Protection System maintenance and testing program. SC's maintenance and testing program states that monthly testing is required on all batteries, but does not refer specifically to temporary batteries.	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, including the temporary battery bank, are continuously monitored and would alarm the control room if any issues were identified. Additionally, the batteries were visually checked each day while operators were doing rounds, and documentation is missing for only two months of monthly battery testing. This issue was related to a single battery bank out of a total of 64 battery banks maintained under SC's Protection System maintenance and testing methodology. Although SC has violated this Standard on three prior occasions, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation appropriately. Following the prior violations, all of which were mitigated by February 2009, SC made changes to its preventative maintenance software to ensure that batteries were tested according to the intervals defined in its Protection System maintenance and testing program, and improved its procedures for keeping and reviewing documentation of maintenance and testing. This issue differs from prior violations because these batteries were temporary in nature and SC personnel were unaware that temporary batteries were subject to the same testing and maintenance procedures as permanent battery installations. The previous violations dealt with permanent battery installations. In addition, the long duration between violations (2008 to 2011) is not indicative of a systemic deficiency in SC's maintenance and testing program.	SC maintained the batteries per its Protection System maintenance and testing program. Additionally, SC revised its maintenance and testing methodology to specifically include temporary battery banks and posted a notice to its field personnel that a revised maintenance and testing program was developed. FRCC verified completion of the mitigation activities.
Midwest Reliability Organization (MRO)	Hennepin County, MN (HCMN)	NCR00381	MRO201100396	PRC-005-1	R1	During a regularly scheduled Compliance Audit, conducted between July 11, 2011 through July 18, 2011, MRO determined that HCMN, registered as a Generator Owner, had an issue with PRC-005-1 R1. HCMN failed to include intervals for maintenance and testing of current transformers (CTs), potential transformers (PTs) and DC control circuitry as required by R1.1. The CTs, PTs and DC control circuitry make up 20% of HCMN's total number of Protection System devices. HCMN also failed to provide a summary of maintenance and testing procedures for all of its Protection System devices in its Protection System maintenance and testing program as required by R1.2.	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 (BPS) because although HCMN failed to document its intervals for CTs, PTs and DC control circuitry, and failed to provide summaries of procedures, HCMN performed a comprehensive review and provided evidence that it maintained and tested its Protection System devices. Additionally, HCMN maintained and tested its Protection System devices more aggressively than industry average. For example, Protection System relays were maintained and tested every three years as opposed to the industry average of six years. Furthermore, HCMN is interconnected to the BPS by 115 kV and has a total generation output of 34 MW.	HCMN revised its Protection System maintenance and testing program to include CTs, PTs, DC control circuitry, and a summary of the procedures. On April 12, 2012, MRO verified that HCMN completed its mitigating activities on March 30, 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
Midwest Reliability Organization (MRO)	Lincoln Electric System (LES)	NCR01001	MRO201100402	PRC-005-1	R2; R2.1	On September 30, 2011, LES, as a Distribution Provider, Generator Owner and Transmission Owner, self-reported an issue with PRC-005-1 R2 for failing to provide maintenance and testing records in accordance with its generation and transmission Protection System maintenance and testing program. Upon receiving the Self-Report, MRO requested that LES perform a comprehensive review of its maintenance and testing records. LES reported that it has approximately 3,043 Protection System devices subject to PRC-005-1 R2, including 431 protective relays, 69 associated communication systems, 2138 voltage and current sensing devices, 42 station batteries and 363 DC control circuits. Of those devices, LES failed to provide evidence that 114 voltage and current sensing devices, 14 station batteries, and 1 DC control circuit, or approximately 4% of its Protection System devices were maintained and tested within the defined intervals.	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 (BPS). Although LES missed visual inspections of current and voltage sensing devices, LES provided evidence that it performed quarterly infrared scans on the devices. Additionally, a subset of the current and voltage sensing devices were monitored continuously on LES's supervisory control and data acquisition system. Furthermore, although LES missed voltage checks for its batteries, LES's generation and substation departments performed other maintenance and testing on the batteries, including cell impedance tests, in accordance with its Protection System maintenance and testing program. In addition, LES only missed the battery voltage checks for two months. Therefore, based on the duration of the tests that were missed and the other tests performed on the devices during the period of issue, MRO determined that this issue only posed a minimal risk to the BPS.	LES performed the following actions to mitigate the issue: (1) performed a comprehensive review of its Protection System maintenance and testing records; (2) performed maintenance and testing on devices lacking records; (3) provided records of maintenance and testing to MRO; and (4) provided training to appropriate staff in an effort to avoid similar issues in the future. On June 1, 2012, MRO verified that LES completed its mitigating activities on May 31, 2012.
Northeast Power Coordinating Council, Inc. (NPCC)	Peabody Municipal Light Plant (PMLP)	NCR07191	NPCC2011008336	PRC-005-1	R1	During a NPCC off-site Compliance Audit on August 26, 2011, it was determined that PMLP, as a Generator Owner, could not provide the required evidence of a satisfactory program for testing of current and potential transformer devices (CT/PTs) and direct current (DC) controls for the GT2 generator Protection System. Testing of these devices was completed during commissioning in 1990. PMLP's Protection System maintenance and testing program interval for testing these devices was during initial installation or replacement, so the testing satisfied the interval as designed by PMLP. However, NPCC determined that PMLP had an issue with the Standard because an interval which only requires testing upon a major event such as initial installation or replacement is not sufficient.	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 there has been no formal testing since commissioning, PMLP had other processes in place to ensure the integrity of these devices. PMLP has an alarming system that monitors the DC trip circuit and DC grounds. The alarm system is monitored by a 24-hour dispatcher. PMLP also performs routine inspection of breaker monitoring lights which, if out, might be indicative of a defective trip coil. PMLP performs routine visual inspections of all CT/PT instrument transformers and an inspection form is filled out. In addition, NPCC considered that the PMLP generating unit is a 52 MW unit and has an average run time of 208.2 hours/year over the last five years.	PMLP completed the following mitigation activities: 1. Tested the CT/PTs at issue; 2. Tested the DC control circuits; 3. Updated the PMLP Protection System maintenance and testing program manual to include defined intervals for regular testing of CT/PTs and DC control circuits. The mitigation activities were verified complete by NPCC.
Reliability*First* Corporation (Reliability*First*)	AES Armenia Mountain Wind, LLC (AES Armenia)	NCR03039	RFC201100857	VAR-002-1.1b	R3	On April 22, 2011, AES Armenia, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to Reliability*First*. AES Armenia reported that on November 4, 2010, at approximately 8:30 a.m. Eastern Standard Time (EST), AES Armenia discovered that the automatic voltage regulator (AVR) was not active. At approximately 9:40 a.m. EST, AES Armenia contacted the Transmission Operator (TOP), notified it of the status change, and restored the AVR to its active mode. AES Armenia later determined that the AVR was inadvertently deactivated when the wind farm management system interface software was reset during a troubleshooting effort the day before. On November 3, 2010, AES Armenia investigated an issue involving greyed-out and frozen data on the Supervisory Control and Data Acquisition (SCADA) system monitor. This investigation revealed that the interface software required a reset, and a manufacturer technician, who did not know that the act of resetting the software would deactivate the AVR, reset the software without reactivating the AVR. AES Armenia discovered the AVR's inactive status the next morning, at which time it contacted its TOP to report the status and propose re-engaging the AVR. Reliability*First* determined that AES Armenia had an issue with VAR-002-1.1b R3 for failing to notify the TOP of a change in status of the AVR within 30 minutes as required by the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. AES Armenia maintained its voltage schedule as set by its TOP at all times for the duration of the remediated issue, and the line voltage never deviated from a +/- 10% band around the control voltage set point. The interconnection between AES Armenia and its TOP is not classified as a Critical Asset by either the TOP or the Regional Transmission Organization (RTO). Additionally, the facts leading up to the issue represent an isolated occurrence.	AES Armenia requested its wind farm management system interface software provider determine the root cause of the software problem and correct it. AES Armenia field-tested the corrected software to ensure its efficacy. AES Armenia also created and implemented a new system operating procedure to verify the status of the AVR, and implemented an automatic email to alert AES Armenia operators of any status change.
Reliability*First* Corporation (Reliability*First*)	Safe Harbor Water Power Corporation (Safe Harbor)	NCR00911	RFC2012010111	VAR-002-1.1b	R1	On September 23, 2011, Safe Harbor, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to Reliability*First*. Reliability*First* determined that the facts and circumstances of the VAR-002-1.1b R3 issue also implicated VAR-002-1.1b R1. Safe Harbor owns and operates twelve hydro generating units. On September 16, 2011, the Safe Harbor operator placed the automatic voltage regulator (AVR) on Unit 10 into manual mode without notifying the Transmission Operator (TOP), as required by VAR-002-1.1b R1.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The AVR for Safe Harbor's Unit 9, which is located on the same plant bus as Unit 10, and the AVRs for Safe Harbor's other units were in automatic mode and were capable of providing voltage support during the relevant time period. In addition, there are alarms in place that sound if the AVR trips to manual mode; however, there is no alarm if the operator switches the AVR into manual mode. Furthermore, Safe Harbor maintained its voltage schedule throughout the duration of the remediated issue, and the voltage for both 230 kV buses to which Safe Harbor is interconnected remained within the operating range during the entire event.	Safe Harbor conducted refresher training on VAR-002 reporting requirements for all station operators and electrical maintenance personnel.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Safe Harbor Water Power Corporation (Safe Harbor)	NCR00911	RFC2011001118	VAR-002-1.1b	R3	On September 23, 2011, Safe Harbor, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to Reliability*First* . Safe Harbor owns and operates twelve hydro generating units. On September 16, 2011, the Safe Harbor operator placed the automatic voltage regulator (AVR) on Unit 10 into manual mode without notifying the Transmission Operator (TOP), as required by VAR-002-1.1b R1. The operator erroneously made this change while attempting to balance VARs among the units. Subsequently, Safe Harbor did not notify its TOP of this status change on the AVR within 30 minutes, as required by VAR-002-1.1b R3.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. The AVR for Safe Harbor's Unit 9, which is located on the same plant bus as Unit 10, and the AVRs for Safe Harbor's other units were in automatic mode and were capable of providing voltage support during the relevant time period. In addition, there are alarms in place that sound if the AVR trips to manual mode; however, there is no alarm if the operator switches the AVR into manual mode. Furthermore, Safe Harbor maintained its voltage schedule throughout the duration of the remediated issue, and the voltage for both 230 kV buses to which Safe Harbor is interconnected remained within the operating range during the entire event.	Safe Harbor conducted refresher training on VAR-002 reporting requirements for all station operators and electrical maintenance personnel.
Reliability*First* Corporation (Reliability*First*)	Detroit Renewable Power LLC (DRP)	NCR11144	RFC2011001117	VAR-002-1.1b	R3	On September 14, 2011, DRP, as a Generator Operator, self-reported an issue with VAR-002-1.1b R3 to Reliability*First* . DRP reported that on July 25, 2011, an automatic voltage regulator (AVR) fuse tripped, causing the AVR to change from automatic mode to manual mode. DRP believed that such changes would cause the generator turbine to stop operating. Because the generator turbine continued to operate, DRP believed that the AVR returned to automatic mode. However, on July 28, 2011, DRP became aware that the AVR had been in manual mode since the fuse trip on July 25, 2011 and immediately contacted its Transmission Operator (TOP) to report the status change.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. DPR continued to control the turbine generator reactive power output in manual mode and maintained its voltage schedule throughout the duration of the remediated issue.	DRP conducted immediate training on the proper procedure for reacting to AVR outages, implemented a bi-annual training schedule for the procedure, added reminders to contact the TOP to turbine and generator alarms on the control room operator stations, and implemented a scheduled strategy session of NERC compliance staff and supervisors to review procedures concerning VAR Reliability Standards.
SERC Reliability Corporation (SERC)	Progress Energy Carolinas (PEC)	NCR01298	SERC2012009742	BAL-005-0.1b	R17	On February 21, 2012, PEC, as a Balancing Authority, self-reported an issue with BAL-005-0.1b R17, stating it had not annually cross-checked its frequency devices against a common reference. PEC reported utilizing five frequency devices at four different locations on its system. SERC reviewed the equipment manuals for these frequency devices and confirmed PEC's statement in the Self-Report that they could not be calibrated. SERC determined that, even though these five frequency devices could not be calibrated, PEC was still required to cross-check the devices against other properly calibrated equipment at least annually. SERC reviewed PEC's records and found that, prior to November 2011, PEC had not annually cross-checked its frequency devices against a common reference. SERC reviewed the results of the cross-check PEC performed against a common reference using historical data from November 10, 2011 and February 23, 2012 and found the devices met the required accuracies.	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. The frequency devices are designed to be maintenance-free and do not require periodic servicing or calibration; and 2. When PEC performed the cross-checks against a common reference, the frequency devices met the required level of accuracy.	SERC verified that PEC completed the following actions: 1. PEC performed a cross-check on all frequency devices used for Area Control Error (ACE) using a common reference, specifically for the five frequency devices at four locations on the PEC system; 2. PEC documented a process for performing the annual cross-check of all PEC frequency devices (primary and back-up) used for ACE against a common reference. The process includes roles and responsibilities and the information needed to perform the tasks; and 3. PEC added an item to the PEC Energy Control Center Scheduler System to notify the appropriate personnel to perform the annual cross-check for all primary and back-up frequency devices at PEC used for ACE.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Progress Energy Carolinas (PEC)	NCR01298	SERC2011008995	INT-001-3	R1	On December 16, 2011, PEC, as a Purchase-Selling Entity, self-reported an issue with INT-001-3 R1, stating that it failed to submit Arranged Interchange for one hour in December 2011. PEC stated that there was actual power flowing on the Dynamic Schedule without an Interchange Transaction Tag (Tag) in place for one hour on December 5, 2011. On February 29, 2012, PEC self-reported an additional issue with INT-001-3 R1, stating that it failed to submit Arranged Interchange for two and a half hours in February 2012. PEC stated that that a Tag was not in place for two and a half hours on February 13, 2012. SERC determined that this issue was related to the December 16, 2011 Self-Report and decided to treat the February 29, 2012 Self-Report as an expansion of scope. PEC has three Dynamic Schedules in place: PJM; East-to-West; and Broad River. PEC has automated some of the Dynamic Schedule Tag production. On December 5, 2011, PEC made a network change on a server/domain controller that runs PEC's PJM dynamic tagging automation. When it made the change, PEC's automated process was suspended from approximately 9:30 p.m. EPT on December 5, 2011 until 1:30 a.m. EPT on December 6, 2011. Prior to the suspension, PEC had already created Tags for the PJM Dynamic Schedule through the hour ending 11:00 p.m. EPT on December 5, 2011. No Tags were created for the remaining two and a half hours of the suspension, but 59 MW of unscheduled power flowed on the PJM Dynamic Schedule through the hour ending midnight on December 6, 2011. The PJM Dynamic Schedule is not a traditional load serving transaction and is designed to always flow in the direction to improve identified congestion points. Therefore, in the event of a transmission loading relief, the power flowing would have been flowing in a direction designed to reduce congestion. PEC issued an After the Fact Tag for the 59 MW that flowed during the hour ending midnight on December 6, 2011. On February 12, 2012, the day shift Transmission Services Desk Operator failed to create the 24-hour profile Tags for the following day, despite an internal PEC process to create next day Dynamic Schedule profiles by 1:00 p.m. EPT daily. This failure affected the East-to-West and the Broad River Dynamic Schedules and resulted in the schedules taking place for two and a half hours with no Tags in place. As a result, 125 MW of unscheduled power flowed on the East-to-West Dynamic Schedule from midnight on February 13, 2012 to 2:30 a.m. EPT on February 13, 2012. At shift change, the next System Operator assumed that the Tags for February 13, 2012 had been created. The Transmission Pricing & Tracking Program alerted the System Operator at 1:55 a.m. EPT on February 13, 2012 that no Tags could be found for the previous hour despite the existence of the Dynamic Schedules for that period. The System Operator responded to the alarm by creating Tags for the East-to-West Dynamic Schedule and the Broad River Dynamic Schedule from 2:30 a.m. EPT through the remainder of the day. The System Operator also created After the Fact Tags for the East-to-West Dynamic Schedule. The Broad River Dynamic Schedule did not have any power flowing during this time frame when the Tag was not in place and therefore did not require an After the Fact Tag.	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 the failures were for short durations and small amounts of power, occurred during off-peak times, and PEC promptly issued After the Fact Tags where necessary.	SERC verified that PEC completed the following actions: 1. PEC developed an enhancement for the Transmission Pricing & Tracking Program validation program to look forward for the presence of future hour tags for all PEC dynamic schedules. If future hour tags have not been created, the system operator will be notified before the future hour so that the system operator can make the necessary manual tag adjustments; 2. PEC reviewed event report findings with system operators; and 3. PEC updated the checklist used by the system operator at the Transmission Service Desk with roles and responsibilities specific to the dynamic tagging process to ensure tags are created as required.
SERC Reliability Corporation (SERC)	South Carolina Electric & Gas Company (SCE&G)	NCR00915	SERC2011007659	MOD-030-2	R1	On July 20, 2011, SCE&G, as a Transmission Service Provider (TSP), self-reported an issue with MOD-030-2 R1, stating it had omitted how it mapped source identification to the model for one independent power producer (IPP) on its system. NERC Reliability Standard MOD-001-1a requires TSPs to select one of three methodologies for calculating Available Transfer Capability (ATC) or Available Flowgate Capability (AFC). If the TSP selects the Flowgate Methodology, the ATC/AFC must be developed in accordance with MOD-030. In addition, the TSP is required to prepare an Available Transfer Capability Implementation Document (ATCID) that includes the information and documentation required by MOD-030. SCE&G adopted the Flowgate Methodology, prepared an ATCID, and filed it with FERC for its review and approval on December 23, 2010. On April 1, 2011, SCE&G implemented the Flowgate Methodology. SCE&G conducted a post-implementation review of its ATCID to ensure compliance with MOD-001-1a and MOD-030-2 and the operational accuracy of the new model. On June 27, 2011, SCE&G confirmed that the model was accurate and complete but the documentation of the model in its ATCID was incomplete. SERC confirmed the omission of the identification and mapping details for one IPP from ATCID Rev. 0 (effective March 31, 2011), specifically for how SCE&G mapped source identification to the model for the IPP. SERC confirmed that the source identification and mapping details for the IPP were included in ATCID Rev. 1 (effective July 18, 2011).	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 although SCE&G's original ATCID did not adequately address MOD-030-2 R1, SCE&G proved that its applicable models associated with this ATCID were complete.	SERC verified that SCE&G updated its ATCID to include a description of the source mapping to the model.

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)	Greenwood Utilities Commission (Greenwood)	NCR01251	SERC2011006619	PRC-008-0	R2	During a SERC Audit, the SERC audit team reported an issue with PRC-008-0 R2 because the audit team's selected sample of the Under Frequency Load Shedding (UFLS) relays presented as evidence by Greenwood did not support the next scheduled completion date of November 2010. SERC found that Greenwood, as a Distribution Provider, failed to test 10 out of 17 UFLS relays (or approximately 59%) by November 2010, as called for in its UFLS maintenance and testing program. Greenwood missed the deadline because it was commissioning a new substation which tied up the contractors who were tasked with testing the UFLS relays.	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. Greenwood's feeder relays are microprocessor-based relays with self-diagnostic capabilities and alarms that are either wired into the station remote terminal unit or a communications processor that is read by the Supervisory Control and Data Acquisition (SCADA) master station. If an alarm is triggered in one of the relays, an audible alarm is sounded in the SCADA system, which identifies the relay that generated the alarm; 2. Test results showed that the UFLS relays were functioning properly, indicating that the UFLS relays likely would have performed their intended functions if called upon to do so; and 3. Greenwood is a small distribution system that has one interconnection point to the BPS through a radial feed from the adjacent system. Greenwood's peak load is approximately 72 MW.	SERC verified that Greenwood tested all of its UFLS relays and found that all of the relays were functioning properly.
Southwest Power Pool Regional Entity (SPP RE)	Independence Power & Light (Independence, Missouri) (INDN)	NCR01072	SPP201000214	FAC-008-1	R1; R1.2.1	During a March 15, 2010 through March 18, 2010 Compliance Audit of INDN, as a Generator Owner (GO), the SPP RE audit team discovered an issue with FAC-008-1 R1.2.1. Specifically, SPP RE discovered that INDN did not address all of its generation facility equipment in its Facility Ratings Methodology (FRM). The FRM addressed all of INDN's transmission facility elements, but for INDN's generation, the FRM stated only that generator Ratings were established based on SPP Criteria 12.1 Rating of Generating Equipment. At the time of the Audit, the SPP Criteria 12.1 Rating of Generating Equipment required the performance of a capacity test to establish generator capability, and did not specifically address the individual operating limits of all generation facility equipment.	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). INDN's FRM had addressed the requirements with regards to INDN's transmission facility elements. However, the INDN's FRM, as it applied to its generation, provided that generators were to be rated according to the SPP Criteria, which provided that generator Ratings would be established by a capacity test, and INDN was performing the capacity tests required by the SPP Criteria. SPP RE determined that the capacity ratings established by capacity tests provided a more accurate rating of INDN's generating facilities compared to other means of rating a facility, such as name-plate rating. Furthermore, at the time of the issue, INDN had a peak load of 315 MW and owned three transmission lines at 100 kV or above. These three lines totaled 23 miles, serving a 46-mile looped 69 kV transmission system. INDN's size (315 MW), coupled with the fact that it had a compliant transmission FRM, and used the SPP Criteria for its generation FRM, reduced the risk posed by INDN's noncompliance with FAC-008-1 R1 to minimal.	INDN revised its generator FRM to address all of the required generator equipment. SPP RE verified completion of the mitigating activities.
Southwest Power Pool Regional Entity (SPP RE)	Independence Power & Light (Independence, Missouri) (INDN)	NCR01072	SPP201000218	TOP-002-2	R11	During a March 15, 2010 through March 18, 2010 Compliance Audit of INDN, as a Transmission Operator (TOP), the SPP RE audit team discovered an issue with TOP-002-2 R11. The SPP RE audit team found that INDN had not been performing current-day or next-day studies to determine its System Operating Limits (SOLs), as required by this Standard. Instead, INDN had relied on studies that Southwest Power Pool (SPP), in its capacity as a NERC registered Reliability Coordinator (RC), performed to monitor the portion of the Bulk Electric System (BES) owned or controlled by its transmission owning member organizations. These studies included next-day and current-day studies. Although INDN had access to these studies, via a website that SPP RC provided, INDN did not have a formal agreement that ensured that INDN would continue to have access to the SPP RC system studies. Furthermore, INDN did not document that it had accessed or reviewed the SPP RC system studies. However, INDN performed summer peak studies, as required.	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 INDN did not document accessing or reviewing the SPP RC system studies, INDN did provide System Operator Duty Checklists, dated as far back as June 2007, that required every shift to review the SPP RC system studies and determine the SOLs accordingly. The checklists provided the hyperlink to review the SPP RC system studies. Furthermore, at the time of the issue, INDN had a peak load of 315 MW and owned three transmission lines at 100 kV or above. These three lines totaled 23 miles, serving a 46-mile looped 69 kV transmission system. In addition, INDN had an experienced group of system operators that has experienced no turnover since 2002, and were capable of addressing issues on the BPS. INDN's size, coupled with its System Operator Duty Checklist requirements to review and assess SPP RC system studies, reduced the risk of INDN's noncompliance with TOP-002-2 R11 to minimal.	As part of the Mitigation Plan, INDN now requests SOLs of common facilities from neighboring utilities on an annual basis. An automated reminder has been setup to make sure coordination of ratings is completed and documented by February 1st of each year. SOLs for transmission and generation facilities are also provided to SPP RC as part of the planning process as requested, but at least annually. INDN now performs N-1, N-2 and specific N-3 Summer/Winter transmission contingency analysis and has developed operating guides for possible operating scenarios to mitigate limit violations. INDN now has an executed, formal agreement with SPP RC, and uses the SPP RC system studies results to comply with TOP-002 R11 requirements, as reported via the SPP OPS1 website. SPP RE verified completion of the mitigating 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)	CenterPoint Energy Houston Electric, LLC (CenterPoint)	NCR04028	TRE201100484	PRC-005-1	R2	CenterPoint, a registered Transmission Owner (TO) and Distribution Provider (DP), submitted a Self-Report on October 17, 2011 regarding a possible issue of PRC-005-1 R2 because two of six maintenance tasks were not performed on 100 of its station batteries. The 100 batteries at issue represent 0.5 % of CenterPoint's total Protection System devices subject to PRC-005. The issue period was from June 18, 2009, when testing was due for the devices, to October 7, 2011, when the issue was mitigated. On September 21, 2011, a CenterPoint crew leader was reviewing documentation for substation tests. During the review of test reports dated September 15, 2011 for the maintenance of the station battery systems at a 345 kV switching station, the crew leader determined that battery inter-cell connection resistance and internal cell impedance tests were not performed. On September 28, 2011, the substation policy consultant and a senior transmission policy consultant in CenterPoint's Transmission Compliance Division reviewed the September 15, 2011 test reports for the 345 kV switching station. During the review, it was determined that specific gravity readings were not included on the test reports. The crew leader confirmed that specific gravity testing had not been performed at the 345 kV switching station and at the 345/138 kV station. On September 29, 2011, the substation policy consultant and the senior transmission policy consultant reviewed additional test reports for station battery systems performed by CenterPoint crews other than the remote two-man crew. All CenterPoint station battery systems, except the four that are the responsibility of the remote two-man crew, are maintained and tested by CenterPoint's Substation Performance Division Diagnostics crews located at the South Houston Complex and the entity's Greenspoint Service Center. The cause of the procedures not being followed by the Diagnostic crews was that legacy maintenance practices, which pre-dated the CenterPoint adoption of its Protection System and UVLS maintenance and testing programs in 2007, were still being utilized for station battery systems. The legacy practices remained in place due to unintentional communication errors that resulted in updated practices not being adequately distributed to the diagnostic crews.	This issue posed a minimum risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the set of 100 station batteries at issue represent 0.5% of CenterPoint's total 18,381 Protection System devices and no performance issues were identified when the missed testing was conducted. Further, the subject devices were continuously monitored during the pendency of the issue, and the missed testing only represented two of the six discrete maintenance tasks of the battery maintenance program. The remaining four maintenance tasks have been performed within the defined intervals, thereby reducing the risk to the BPS. All test results were within normal parameters, indicating the batteries were capable of performing and, in fact, did perform as designed.	The missed testing was completed on October 6-7, 2011 and CenterPoint completed a supplemental five-phase Mitigation Plan on March 21, 2012 to bring the facilities at issue in compliance with this Standard. Phase 1 transferred the responsibility for the maintenance of the station battery systems for the 345 kV switching station and the 345/138 kV station from the remote two-man crew to Substation Performance Division's Diagnostics crews located at a Service Center. Phase 2 performed the following testing: battery inter-cell connection resistance testing and internal cell impedance testing at the 345 kV switching station and the 345/138 kV station; specific gravity testing on all battery cells at applicable stations. Phase 2a performed the following tasks: modified 39 applicable battery sets to allow for inter-cell connection resistance testing and internal cell impedance testing; performed inter-cell connection resistance testing and internal cell impedance testing on applicable battery sets. Phases 3 and 3a reinforced the knowledge of all of the Substation Performance Division's Diagnostic crews on specific maintenance and testing tasks. Phase 4 implemented an on-line test records software program for the tasks associated with battery maintenance and testing and verified it was performing as expected. Phase 5 included contacting the applicable battery manufacturers regarding possible modifications to their product that would eliminate the need for field modifications. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	The Dow Chemical Co (Dow Chemical)	NCR04146	TRE201100513	VAR-002-1.1b	R3.1	On October 28, 2011, Dow Chemical, as a Generator Operator (GOP), self-reported that it was not in compliance with VAR-002-1b R3.1. The remediated issue began on December 20, 2010, when during the course of intermittent generator exciter issues, the Automatic Voltage Regulator (AVR) on one of Dow Chemical's generator units at its Freeport facility automatically switched from automatic to manual status. Dow Chemical did not report that change in status to its Transmission Operator (TOP) within 30 minutes, as required by this Standard. Dow Chemical's Freeport plant site has 15 generating units that have a combined nameplate rating of 1,938 MVA. The issue ended on December 28, 2010, when a report was made to the TOP concerning these events.	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 Dow Chemical's power system voltages, including generator bus voltage, were monitored by Distributed Control Systems (DCS) and Supervisory Control and Data Acquisition (SCADA) systems. Also, there were multiple alarm systems for voltage deviations from defined ranges in Dow Chemical's powerhouse and power dispatch centers. Both of these locations are manned 24 hours a day. Moreover, the unit at issue, which has a nameplate rating of 227.5 MVA, and the other units of Dow Chemical's generation system are mainly used for self-supply. During the duration of the issue, Dow Chemicals did not export any power to the BPS, and for all of 2010, Dow Chemical only exported energy equal to 1% of total energy that it bought. In 2011, Dow Chemical only exported energy equal to 6.9% of total energy that it bought. And, for the times that Dow Chemical injects power into the Electric Reliability Council of Texas' system, there are several other generating units nearby that would have compensated for the unit's lack of response due to its AVR being switched to manual status.	Dow Chemical reported the status change on December 28, 2010. AVR status signals for all generators located at the Freeport site have been automated with direct status information, which is continuously transferred to the Dow Chemical's Qualified Scheduling Entity (QSE), which communicates the status information to the TOP. This allows for immediate notification to the TOP without depending on Dow Chemical's operating personnel to immediately recognize the VAR002-1.b R3.1 compliance requirements. The QSE has a contractual obligation to report such information to the TOP in a timely manner. Also, all AVR status alarms have been relocated to a central Power Dispatch Center (previously only alarmed in each Power House), a system designed to prompt verbal notification of AVR status, including expected duration, to Dow Chemical's QSE, in addition to the automated system. Texas RE verified completion of these mitigating 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)	Sacramento Municipal Utility District (SMUD)	NCR05368	WECC2012009686	VAR-002-1.1b	R3.1	On February 9, 2012, SMUD, as a Generator Operator (GOP), self-reported an issue with VAR-002-1.1b R3.1. SMUD's Campbell Steam Turbine Generator #1 (STG1) has a primary automatic voltage regulator (Primary AVR) and a secondary automatic voltage regulator (Secondary AVR). STG1 is equipped with a power system stabilizer (PSS) when operating with the Primary AVR in service, but is not equipped with a PSS when operating with the Secondary AVR in service. On December 12, 2011, SMUD conducted planned, routine 5-year generator testing. During the generator testing on STG1, SMUD identified STG1 operating with its Secondary AVR in service. SMUD conducted an internal investigation regarding the root cause of STG1 operating in Secondary AVR rather than Primary AVR. SMUD's compliance department determined the plant operator placed the Secondary AVR into service as part of a testing protocol by the system vendor. SMUD could not identify in its log books associated with STG1 an indication that the plant notified the Transmission Operator (TOP). WECC reviewed SMUD's Self-Report and determined SMUD did not notify the TOP of a change in the status of the PSS within 30 minutes of the change in status and did not provide an estimated time when it would return to service. Accordingly, WECC determined SMUD had a possible issue with VAR-002-1.1b R3.1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because STG1 is a steam generator part of a combined cycle unit with a capacity of 55 MW that had a capacity factor in 2010 of 45.6% and a capacity factor in 2011 of 31.5%. The generator connects to the system between the Pocket and Hedge 230 kV substations which is a networked area of 230 kV lines. In this area, the effect of the TOP not knowing the status of the PSS on a unit of this size is negligible. The amount of generation, particularly with this capacity factor, is a fraction of the generation available at the plant and an even smaller fraction of the generation available to the TOP.	SMUD clarified the naming conventions on its AVR (specifically on the voltage regulator cabinet) selectors to remove the specific cause of the error. SMUD re-wrote its steam turbine operating procedure, inspection of watch procedure, start-up & shutdown checklists, work management. SMUD also created a NERC quick reference-card to identify and include reporting requirements associated with NERC Reliability Standards. SMUD implemented a logic change in its plant Distribution Control System to signal ("PSS On") to both TOP personnel and site personnel as applicable. SMUD made this change because if a discrete problem happens again, the "PSS On" indication will go off and activate a "PSS Off" alarm in the appropriate control room. SMUD also included training as part of its mitigation activities: SMUD staff provided training to all Sacramento Power Authority (SPA) Cogen III personnel on NERC VAR-002-1.1b requirements and SMUD notified all plant managers to review and reinforce the notification requirements associated with this requirements with generation plant operating personnel.
Western Electricity Coordinating Council (WECC)	Las Vegas Power Company, LLC (LVPC)	NCR05215	WECC2012009962	VAR-002-1.1b	R3	On March 29, 2012, LVPC, as a Generator Operator and a Generator Owner, submitted a Self-Report for an issue with NERC Reliability Standard VAR-002-1.1b R3. To comply with R3 of the Standard, LVPC, as the Generator Operator and Generator Owner, is required to notify its associated Transmission Operator (TOP), Seattle City Light (SCL), within 30 minutes of a status or capability change on any generator Reactive Power resource, including the status of each automatic voltage regulator and power system stabilizer (PSS), and the expected duration of the change in status or capability. According to the Self-Report, on January 13, 2012, during maintenance of its MARK V control system, the PSS switched to "off" on LVPC's generator GT1A, without manual command or operator knowledge. Due to the original design and configuration of the MARK V control system, there was no audio or visual alarm to notify plant personnel of the change in status. On January 17, 2012, LVPC plant personnel notified the TOP that it had discovered the GT1A PSS was out of service during the period from January 13, 2012 to January 17, 2012, and LVPC immediately returned to it service upon discovery on January 17, 2012. Because the change in status was not identified until January 17, 2012, notification was provided to the TOP outside of the 30 minutes required under the Standard. WECC determined that LVPC has an issue of VAR-002-1.1b R3, for failing to notify the TOP of a change in PSS status, outside the 30 minutes 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 because the generator involved has a capacity of 165 MW and is located at a generation facility with two other generators providing additional output capacity of 395 MW, and within five miles of another 2,000 MW of generation. Because this generation with PSS is available in the immediate vicinity, it minimizes the need for system damping and tends to compensate for possible undesirable behavior of the generator in scope.	LVPC notified its TOP that it had resumed operation of its generator with PSS in service to provide reactive and voltage control. LVCP will add audio and visual alarms to notify personnel when the PSS is off.
Western Electricity Coordinating Council (WECC)	Las Vegas Power Company, LLC (LVPC)	NCR05215	WECC2012009963	VAR-501-WECC-1	R1	On March 29, 2012, LVPC submitted a Self-Report for an issue with NERC Reliability Standard VAR-501-WECC-1 R1. To comply with R1 of the Standard, LVPC, as the Generator Operator, is required to have its power system stabilizer (PSS) in service 98% of all operating hours for synchronous generators equipped with PSS. According to the Self-Report, the PSS was out of service on LVPC's generator GT1A for 25.4 hours during the period from January 13, 2012 through January 17, 2012, excluding hours of non-operation that are exempt from the calculation, based on the exceptions in R1.1 through R1.12 of the Standard. During this period, the plant experienced a MARK V control system component failure. Enforcement determined that LVPC has an issue with VAR-501-WECC-1 R1, for its failure to have its PSS in service 98% of all operating hours for its synchronous generators equipped with PSS for the period from January 13, 2012 to January 17, 2012, LVPC experienced a MARK V control system component failure. Initial repairs took place on January 10, 2012, January 12, 2012, January 13, 2012 and January 15, 2012. According to the Standard, the PSS may be out of service up to 60 consecutive days for repair per incident of component failure. WECC determined LVPC had 25.4 hours, accumulated between January 16, 2012 (17.07 hours) and January 17, 2012 (8.33 hours) over and above the exemption allowed in R1.8, for component failure. Because GT1A was electrically connected for a total of 610.26 hours during the first quarter of 2012, the 25.4 hours is divided by 610.26 hours (the number of hours the generator was in service for the quarter); equaling 4.16% PSS unavailability, or a PSS in service percentage of 95.84%.	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 amount of time the generator operated with the PSS off was approximately 25 hours. Additionally, the generator involved has an output capacity of 165 MW and is located at a generation facility with two other generators providing additional output capacity of 395 MW, and within five miles of another 2,000 MW of generation. Because this generation with PSS is available in the immediate vicinity, it minimizes the need for system damping and tends to compensate for possible undesirable behavior of the generator in scope.	LVPC revised its startup procedures to include a checklist that requires the operator to verify that the PSS is enabled by January 30, 2012; added PSS status to the operator's Inspection of Watch form that is performed twice each shift by January 30, 2012; and added audio and visual alarms in cases where the PSS is off, by April 30, 2012. WECC issued a Notice of Mitigation Plan Acceptance on June 7, 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
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200800886	PER-001-0	R1	On June 30, 2008, following an internal review of its compliance program stemming from its registration on the NERC Compliance Registry on May 14, 2008 as a Transmission Operator (TOP), NNSAL submitted a Self-Report addressing noncompliance with PER-001-0 R1. Specifically, NNSAL reported that its current dispatcher job description did not contain the authority to implement real-time actions to ensure the stable and reliable operation of the bulk power system (BPS). While NNSAL's dispatcher job description did not provide the written authority for its operating personnel to implement real-time actions, these responsibilities and authorities were identified and communicated through internal trainings on the NNSAL transmission system. Specifically, NNSAL's training and certificate requirements call for operating personnel to be capable of handling situations which involve real-time actions including normal or emergency conditions. Although NNSAL had the appropriate training in place to provide operating personnel with the responsibility and authority to implement real-time actions, and these responsibilities and authorities are understood by the operating personnel, it did not separately and specifically address that authority through the dispatcher job description.	This issue did not pose a serious or substantial risk and only posed minimal risk to the reliability of the BPS. Although NNSAL did not formally document its dispatcher's authority to implement real-time actions, the authority was disseminated through the NNSAL operating training plans. As a result, the NNSAL dispatcher was prepared and trained to respond to take or direct timely and appropriate real-time actions.	NNSAL revised the authority and responsibilities of the job description of its dispatcher position, including specific statements to address dispatcher authority required to take real-time actions during normal and emergency conditions.
Western Electricity Coordinating Council (WECC)	Milford Wind Corridor Phase I, LLC (MILW)	NCR10394	WECC2012009495	PRC-005-1	R2	On January 20, 2012, MILW, as a Transmission Owner (TO), self-certified noncompliance with PRC-005-1 R2. MILW verified the status of the digital inputs and outputs and all of the voltage and current inputs of the Protection System equipment every six months according to its generation maintenance and testing program. MILW's facility went commercial in 2009 and the first two six-month tests were completed on schedule. However the third six-month test was missed so that a year passed before the next six-month test was done. WECC concluded that MILW was in noncompliance with PRC-005-1 R2.	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 MILW had maintained and tested all its protection equipment within their defined intervals, with the exception of this single test involved in this issue. In addition, Milford tested and maintained the equipment involved in this issue six months after the missed test.	This issue was effectively mitigated when Milford tested and maintained the protection equipment involved in this issue six months after it missed the test resulting in the issue.
Western Electricity Coordinating Council (WECC)	Western Area Power Administration - Desert Southwest Region (WALC)	NCR05461	WECC200801290	BAL-005-0	R17	On October 24, 2008, WECC conducted a Compliance Audit of WALC and discovered an issue with BAL-005-0 R17. To comply with the Standard, WALC, as a Balancing Authority (BA), shall at least annually check and calibrate its time error and frequency devices against a common reference. The Audit Team found that WALC uses TrueTime Model XL-DC-600 Time and Frequency Receivers for primary and backup frequency measurement with time and frequency monitor modules. During the Audit, WALC personnel stated that these devices continuously check and calibrate themselves against Global Positioning System (GPS) Clock signals. The TrueTime technical manual states that these devices cannot be calibrated by the user, and that the time error signal is referenced to a common external universal time source via GPS satellite links. The TrueTime Model XL-DC-600 Time and Frequency Receivers that WALC uses meet the Standard's .001 Hz accuracy requirement. There is an associated, approved NERC interpretation of this Standard, which states that "Some devices used for time error and frequency measurement cannot be calibrated as such. In this case, these devices should be cross-checked against other properly calibrated equipment and replaced if the devices do not meet the required level of accuracy." A follow-up interview with WALC personnel revealed that WALC does not cross-check these devices against any other properly calibrated devices. Therefore, WECC determined WALC had an issue with BAL-005-0 R17 because WALC had not cross-checked its time error and frequency devices against properly calibrated devices.	This issue did not pose a serious or substantial risk and only posed minimal risk to the reliability of the bulk power system (BPS) because the frequency device used by WALC is not designed to be calibrated and is manufactured to meet a .001 Hz accuracy requirement. Additionally, the time and frequency source is referenced to a GPS time reference. Total failure of the device would be immediately apparent to WALC personnel based on displayed accumulated time error.	WALC mitigated this issue immediately upon discovery. WALC cross checked the TrueTime devices against independent, calibrated devices. WALC submitted a Certification of Accuracy to demonstrate the cross-check and to further demonstrate the devices were operating in an accurate state. WALC has procedure in place to ensure annual completion of this calibration according to the Standard.
Western Electricity Coordinating Council (WECC)	Bonneville Power Administration (BPA)	NCR05032	WECC201102941	MOD-029-1a	R8	On September 1, 2011, BPA, as a Transmission Service Provider, submitted a Self-Report citing an issue with MOD-029-1a R8. Specifically, BPA reported that on August 9, 2011, BPA calculated the Total Transfer Capabilities (TTC), but that due to a database locking issue, BPA's Available Transfer Capabilities (ATC) Calculation System failed to upload the TTC values into the non-firm Available Transfer Capability for the ATC Path for that period (ATCNF) formula for Hours Ending (HE) HE01 through HE07, HE10 through HE11, and HE13. Instead, the system used "default" TTC values. Once BPA discovered the problem, BPA reported that it contacted its software vendor and remediated the problem that same day. WECC reviewed BPA's Self-Report. WECC determined that BPA failed to include accurate TTC values in its calculation of ATCNF for ten hours on August 9, 2011 and determined that the issue period spanned ten hours.	WECC determined that this issue did not pose a serious or substantial risk and only posed minimal risk to the reliability of the bulk power system (BPS). BPA set up its system to use the R8 algorithm. Because of database locking issues, however, the system could not access the calculated TTC values. In addition, BPA promptly discovered and remediated the issue. The scope of the issue was limited to a single path. The duration of the issue was limited to ten hours on August 9, 2011. The defaulted TTC value did not radically alter ATCNF calculation during the issue period.	BPA contacted OATI, the system vendor. OATI reinitialized the appropriate systems to re-process TTCs for the ATC N to S Path and push them correctly through to the ATC Calculation System so that the problem would not continue from that point forward.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO2012010158	CIP-004-3	R4; R4.1	MRO_URE1 self-reported an issue with CIP-004-3 R4 for failing to revoke a contractor's unescorted physical access to two substations containing Critical Cyber Assets (CCAs) within seven days. The contractor did not provide MRO_URE1 with a timely notification of a change in its personnel. The contractor's access was not revoked within the seven calendar days required by the Standard due to a misunderstanding. The contractor incorrectly thought that taking possession of the individual's badge would revoke access; however, access to both substations is controlled by a combination of personal identification numbers and biometrics, and not just a badge.	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. The contractor's training and personnel risk assessment were both current. In addition, this was an isolated incident. MRO_URE1 reviewed its access records and did not identify any other instances of unauthorized access. Furthermore, the contractor's access privileges were not used during the period between voluntary termination and revocation, and the contractor did not have electronic access to MRO_URE1's CCAs.	MRO_URE1 revoked the contractor's access privileges. MRO verified that MRO_URE1 completed its mitigating activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO2012009921	CIP-007-3	R4; R4.2	MRO_URE2 self-reported an issue with CIP-007-3 R4.2 for failing to keep anti-virus and malware prevention signatures updated on several Cyber Assets, which were Critical Cyber Assets (CCAs). Specifically, these Cyber Assets made up 11% of MRO_URE2's total CCAs. The Cyber Assets were being retired from the system, but had not been removed from the network when they were replaced. MRO_URE2's malicious software prevention policy required monthly checks for new virus signatures. For one month, MRO_URE2 did not perform a monthly check for the retired devices.	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 because only 11% of MRO_URE2's total CCAs were affected, those devices were being retired from MRO_URE2's system and were not actively used. Additionally, MRO_URE2 only missed the anti-virus signature update by 18 days. The devices were protected in accordance with all of the other applicable CIP requirements.	MRO_URE2 removed the Cyber Assets from its system. MRO verified that MRO_URE2 completed its mitigating activities.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001002	CIP-007-3	R9	RFC_URE1 self-reported an issue with CIP-007-3 R9. RFC_URE1 changed its anti-virus software on all of its Critical Cyber Assets (CCAs). RFC_URE1 discovered that it had not updated its cybersecurity procedure within thirty calendar days of the change pursuant CIP-007-3 R9. Reliability*First* determined that RFC_URE1 had an issue with CIP-007-3 R9 for failing to document a change resulting from the modifications to its anti-virus system within thirty calendar days of RFC_URE1 completing the change.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). This risk to the reliability of the BPS was mitigated by the fact that at all times RFC_URE1's Cyber Assets and CCAs were protected by anti-virus software. In addition, the issue incident was an isolated incident in which RFC_URE1 did not follow its documented cybersecurity procedure.	RFC_URE1 performed additional training on all staff engaged in managing Cyber Assets within the Electronic Security Perimeter on its cybersecurity procedure. RFC_URE1 also included, in its additional training, an emphasis on the need to update all relevant documentation within the required timeframe.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001047	CIP-006-2a	R1; R1.2	RFC_URE1 self-reported an issue with CIP-006-2a R1.2. Prior to mandatory compliance with Reliability Standard CIP-006-2a R1, RFC_URE1 installed a steel cage in the ceiling of its transmission control room to create a completely enclosed six-wall border. Upon further examination, RFC_URE1 determined that the way in which the steel cage was installed allowed for access into the transmission control room from the ceiling above. Reliability*First* determined that RFC_URE1 had had an issue with CIP-006-2a R1 for not identifying this physical access point or taken measures to control entry at that access point.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability to the BPS was mitigated by the following factors. RFC_URE1's transmission control room is located within RFC_URE1's generation control room, which is locked at all times with cipher locks (key pad devices that require a specific code to be entered before authorizing access), the combination of which is only given to individuals who have received authorization from RFC_URE1. Additionally, RFC_URE1 monitors access to the transmission control room with security cameras.	RFC_URE1 installed the equipment necessary to create a complete six-wall border surrounding its transmission control room that eliminates the access point into the transmission control room from the ceiling above.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001071	CIP-005-3a	R5; R5.3	RFC_URE1 self-reported an issue with CIP-005-3a R5.3. RFC_URE1 determined that it had not retained electronic access logs for at least 90 calendar days. Specifically, RFC_URE1 discovered that as the result of a service outage of its primary centralized log server, the primary centralized log server was not retaining access logs.	Reliability*First* determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. RFC_URE1 was collecting logs and sending alerts through its backup centralized log server during the duration of the remediated issue; however, the backup log server only retained access logs for 30 calendar days, rather than the required 90 days. RFC_URE1 was still logging access to the applicable devices and appropriate personnel still received alerts from the backup centralized log server. Additionally, RFC_URE1 did not detect any security incidents through the backup centralized log server during the duration of the remediated issue.	RFC_URE1 configured the settings on its centralized server to retain access logs for 90 calendar days.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001072	CIP-007-3	R6; R6.4	RFC_URE1 self-reported an issue with CIP-007-3 R6.4. RFC_URE1 determined that it had not retained all system security logs related to its system that monitors all network devices and acts as RFC_URE1's system log based network performance monitoring software, for at least 90 calendar days. Specifically, RFC_URE1 discovered that as the result of a service outage of its primary centralized log server, it was not retaining access logs for the required 90 days.	Reliability*First* determined this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the following factors. Through a backup centralized log server, RFC_URE1 retained all logs required by CIP-007-2a R6 for 30 calendar days. Also, RFC_URE1 was performing real time logging for access to the applicable devices and appropriate personnel received alerts from the backup centralized log server during the duration of the remediated issue. Additionally, RFC_URE1 did not detect any security incidents through the backup centralized log server and review of the logs for the duration of the remediated issue.	RFC_URE1 configured the settings on its centralized server to retain access logs for 90 calendar days.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1) CER-Colorado Bend Energy Partners LP (Colorado Bend)	NCRXXXXX	TRE201100523	CIP-002-2	R1	During a Spot-Check, Texas RE concluded that Texas RE_URE1 did not have adequate documentation of a risk-based assessment methodology (RBAM) to use to identify Critical Assets (CAs) at a newly purchased station, as required by CIP-002-2 R1. Texas RE_URE1 had an issue with this Standard for a period of four months, after acquiring the station and registering with NERC. Texas RE_URE1 conducted a high-level review shortly after acquiring the station and concluded that it had no CAs or Critical Cyber Assets (CCAs). However, Texas RE_URE1 used a RBAM that applied to other assets from its fleet to identify CAs and CCAs at this station. Texas RE_URE1 also concluded that it needed to update the RBAM created by the previous station owner to reflect the requirements included in its current fleet program and to fully address this Standard. Texas RE_URE1 also mistakenly concluded it had two years to update its RBAM. Texas RE_URE1 documented an acceptable RBAM that addressed the requirements of this Standard four months after its registration. Therefore, Texas RE determined that the start date of the issue was the date of Texas RE_URE1's registration with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE1 realized that it needed to update its RBAM, and that it had no CAs or CCAs, but failed to update its RBAM for four months. Also, during the pendency of the issue, Texas RE_URE1 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility and determined that it had no CAs or CCAs. After Tex as RE_URE1 documented an RBAM that addressed the requirements of this Standard, and applied the updated RBAM, it identified no CAs or CCAs at the facility at issue. In addition, the duration of this remediated issue was limited to four months. Because the risk to the BPS was mitigated by the existence of an RBAM at the time of the issue, although not fully compliant with this Standard, because there were no CAs and CCAs during the pendency of the issue or thereafter, and because the issue lasted for four months, Texas RE determined this issue presented a minimal risk to the BPS.	Texas RE_URE1 updated the RBAM for the facility at issue to address the requirements of this Standard. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1) CER-Colorado Bend Energy Partners LP (Colorado Bend)	NCRXXXXX	TRE201100524	CIP-002-2	R2	During a Spot-Check, Texas RE concluded that Texas RE_URE1 did not develop a list of its identified Critical Assets (CAs) determined through an annual application of the risk-based assessment methodology (RBAM), as required by CIP-002-2 R2. Texas RE_URE1 conducted a high-level review of a newly acquired station-shortly after acquiring the station and registering with NERC. Texas RE_URE1 used a RBAM that applied to other assets from its fleet to identify CAs and Critical Cyber Assets (CCAs) within its station, determined that it had no CAs and CCAs but failed to document its findings. However, the list of identified CAs and CCAs created by the previous owner of the station was redacted and therefore unreadable, thus presenting an issue with CIP-002-2 R2. This noncompliant list was in place for four months until Texas RE_URE1 documented an updated RBAM for its newly acquired station, and used the RBAM to develop a list of its CAs, which addressed the requirements of CIP-002-2 R2. Texas RE determined that the start date of the issue was the date of Texas RE_URE1's registration with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE1 realized that it needed to update its RBAM, and that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs, as required by this Standard. Also, the duration was limited to four months. After applying the updated RBAM, Texas RE_URE1 confirmed and documented that there were no CAs or CCAs at the facility at issue. Also, during the pendency of the issue, Texas RE_URE1 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE1 updated the RBAM for the facility at issue and created a list of CAs applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1) CER-Colorado Bend Energy Partners LP (Colorado Bend)	NCRXXXXX	TRE201100525	CIP-002-2	R3	During a Spot-Check, Texas RE concluded that Texas RE_URE1 did not develop a list of associated Critical Cyber Assets (CCAs) essential to the operation of the Critical Assets (CAs), as required by CIP-002-2 R3. Texas RE_URE1 conducted a high-level review of a newly acquired station shortly after purchasing the station and registering with NERC. Texas RE_URE1 used a risk-based assessment methodology (RBAM) that applied to other assets from its fleet to identify CAs and CCAs within its station, determined that it had no CAs and CCAs but failed to document its findings. However, the list of identified CAs and CCAs created by the previous owner of the station was redacted and therefore unreadable, thus presenting an issue with CIP-002-2 R2. This noncompliant list was in place for four months until Texas RE_URE1 documented an updated RBAM for its newly acquired station, and used the RBAM to develop a list of CCAs, which addressed the requirements of CIP-002-2 R3. Texas RE determined that the start date of this issue was from the date of Texas RE_URE1's registration with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE1 realized that it needed to update its RBAM, and that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs, as required by this Standard. Also, the duration was limited to four months. After applying the updated RBAM, Texas RE_URE1 determined that there were no CAs and CCAs at the facility at issue. Also, during the pendency of the issue, Texas RE_URE1 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE1 updated the RBAM for the facility at issue and created a list of CAs and CCAs by applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE verified completion of these mitigating 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)	Unidentified Registered Entity 1 (Texas RE_URE1) CER-Colorado Bend Energy Partners LP (Colorado Bend)	NCRXXXXX	TRE201100526	CIP-002-2	R4	During a Spot-Check, Texas RE concluded that Texas RE_URE1 did not keep a signed and dated record of the senior manager or delegate(s)' annual approval of the risk-based assessment methodology (RBAM), the list of Critical Assets (CAs) and the list of Critical Cyber Assets (CCAs), as required by CIP-002-2 R4. Texas RE_URE1 conducted a high-level review of a newly acquired station shortly after purchasing the station and registering with NERC. Texas RE_URE1 used a RBAM that applied to other assets from its fleet to identify CAs and CCAs within its new station, determined that it had no CAs and CCAs but failed to document its findings. This noncompliant RBAM was used for four months until Texas RE_URE1 documented an updated RBAM for its newly acquired station, and used the updated RBAM to develop lists of CAs and CCAs. The updated RBAM, and lists of CAs and CCAs was approved by the senior manager or delegates four months after Texas RE_URE1 purchased the station and registered with NERC. Texas RE determined that the start date of this issue was the date of Texas RE_URE1's registration with NERC to the date an updated RBAM and lists of CAs and CCAs were created and approved by the senior manager.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the issue was documentation in nature as Texas RE_URE1 realized that it needed to update its RBAM, and that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs, and to keep a record of the senior manager's approval of these documents, as required by this Standard. After applying the updated RBAM, Texas RE_URE1 determined that there were no CAs and CCAs at the facility at issue, and the senior manager or delegates approved the RBAM and the null lists of CCAs and CAs. Also, during the pendency of the issue, Texas RE_URE1 had a RBAM in place that was also applicable to other assets, performed a high-level review of this particular facility and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE1 updated the RBAM for the facility at issue and created a list of CAs and CCAs applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE_URE1's senior manager approved the RBAM and lists of CAs and CCAs. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1) CER-Colorado Bend Energy Partners LP (Colorado Bend)	NCRXXXXX	TRE201100527	CIP-003-2	R2	During a Spot-Check, Texas RE concluded that Texas RE_URE1 did not assign a single manager with overall responsibility and authority for leading and managing Texas RE_URE1's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2, as required by CIP-003-2 R2. Texas RE determined that when Texas RE_URE1 first registered with NERC, it properly assigned a single manager, as per CIP-003-2 R2. However another person, who was not the delegated single manager, approved Texas RE_URE1's updated risk-based assessment methodology (RBAM), the list of Critical Assets (CAs) and the list of Critical Cyber Assets (CCAs). Texas RE_URE1 realized the discrepancy and prepared documentation, stating that the person who approved the RBAM and the list of CAs and CCAs was in fact the proper, delegated manager and had authority to approve these documents. Texas RE determined that because a person other than the initially authorized single manager signed the RBAM and list of CAs and CCAs, Texas RE_URE1 was noncompliant with CIP-003-2 R2. Texas RE determined that the issue duration was for a period of about three months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Texas RE_URE1 had a senior manager with overall responsibility for compliance with CIP-002-2 through CIP-009-2 at all times. However, for the period of about three months the delegation of authority to a single senior manager with overall responsibility existed but was not documented. Texas RE determined that this issue was documentation in nature, thereby reducing the risk to the BPS to minimal.	Texas RE_URE1 documented the delegation of authority to a single senior manager. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) CER-Quail Run Energy Partners LP (Quail Run)	NCRXXXXX	TRE201100530	CIP-002-2	R1	During a Spot-Check, Texas RE concluded that Texas RE_URE2 did not have adequate documentation of a risk-based assessment methodology (RBAM) to use to identify Critical Assets (CAs) at a newly purchased station, as required by CIP-002-2 R1. Texas RE_URE2 was noncompliant with this Standard for a period of four months, after purchasing the station and registering with NERC. Texas RE_URE2 conducted a high-level review shortly after acquiring the station and concluded that it had no CAs or Critical Cyber Assets (CCAs). However, Texas RE_URE2 used a RBAM that applied to other assets from its fleet to identify CAs and CCAs at this station. Texas RE_URE2 also concluded that it needed to update the RBAM created by the previous station owner to reflect the requirements included in its current fleet RBAM and to fully address this Standard. Texas RE_URE2 also mistakenly believed that it had two years to update its current RBAM. Texas RE_URE2 documented an acceptable RBAM that addressed the requirements of this Standard four months after its registration with NERC. Therefore, Texas RE determined that the issue duration was from the date Texas RE_URE2 was registered with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE2 realized that it needed to update its RBAM, and that it had no CAs or CCAs, but failed to update its RBAM for four months. Also, during the pendency of this issue, Texas RE_URE2 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility and determined that it had no CAs or CCAs. After Texas RE_URE2 documented a RBAM that addressed the requirements of this Standard, and applied the updated RBAM, it identified no CAs or CCAs at the facility at issue. In addition, the duration of this remediated issue was limited to four months. Because the risk to the BPS was mitigated by the existence of an RBAM at the time of the issue, although not fully compliant with this Standard, because there were no CAs and CCAs during the pendency of the issue or thereafter, and because the issue lasted for four months, Texas RE determined this issue presented a minimal risk to the BPS.	Texas RE_URE2 updated the RBAM for the facility at issue when a senior manager approved the RBAM. Texas RE verified completion of these mitigating 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)	Unidentified Registered Entity 2 (Texas RE_URE2) CER-Quail Run Energy Partners LP (Quail Run)	NCRXXXXX	TRE201100531	CIP-002-2	R2	During a Spot-Check, Texas RE concluded that Texas RE_URE2 did not develop a list of its identified Critical Assets (CAs) determined through an annual application of the risk-based assessment methodology (RBAM), as required by CIP-002-2 R2. Texas RE_URE2 conducted a high-level review of a newly acquired station shortly after purchasing the station and registering with NERC. Texas RE_URE2 used a RBAM that applied to other assets from its fleet to identify CAs and Critical Cyber Assets (CCAs) within its new station, determined that it had no CAs and CCAs but failed to document its findings. However, the list of identified CAs and CCAs created by the previous owner of the station was redacted and therefore unreadable, thus presenting an issue with CIP-002-2 R2. This noncompliant list was in place for four months until Texas RE_URE2 documented an updated RBAM for its newly acquired station, and used the RBAM to develop a list of its CAs, which addressed the requirements of CIP-002-2 R2. Texas RE determined that the issue was from the date of Texas RE_URE2's registration with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE2 realized that it needed to update its RBAM, that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs, as required by this Standard. Also, the duration of this issue was limited to four months. After applying the updated RBAM, Texas RE_URE2 determined that there were no Critical Assets at the facility at issue. Also, during the pendency of the issue, Texas RE_URE2 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility, and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE2 updated the RBAM for the facility at issue and created a list of CAs applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) CER-Quail Run Energy Partners LP (Quail Run)	NCRXXXXX	TRE201100532	CIP-002-2	R3	During a Spot-Check, Texas RE concluded that Texas RE_URE2 did not develop a list of associated Critical Cyber Assets (CCAs) essential to the operation of the Critical Assets (CAs), as required by CIP-002-2 R3. Texas RE_URE2 conducted a high-level review of a newly acquired station shortly after purchasing the station and registering with NERC. Texas RE_URE2 used a risk-based assessment methodology (RBAM) that applied to other assets from its fleet to identify CAs and CCAs within its new station, determined that it had no CAs and CCAs but failed to document its findings. However, the list of identified CAs and CCAs created by the previous owner of the station was redacted and therefore unreadable, thus presenting an issue with CIP-002-2 R2. This noncompliant list was in place for four months until Texas RE_URE2 documented an updated RBAM for its newly acquired station, and used the RBAM to develop a list of CCAs, which addressed the requirements of CIP-002-2 R3. Texas RE determined that the issue was from the date of Texas RE_URE2's registration with NERC to the date an updated RBAM was created and approved.	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 documentation in nature as Texas RE_URE2 realized that it needed to update its RBAM, that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs, as required by this Standard. Also, the duration was limited to four months. After applying the updated RBAM, Texas RE_URE2 determined that there were no CAs and CCAs at the facility at issue. Also, during the pendency of the issue, Texas RE_URE2 had a RBAM in place that was also applicable to other assets, and performed a high-level review of this particular facility, and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE2 updated the RBAM for the facility at issue and created a list of CAs and CCAs applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) CER-Quail Run Energy Partners LP (Quail Run)	NCRXXXXX	TRE201100533	CIP-002-2	R4	During a Spot-Check, Texas RE concluded that Texas RE_URE2 did not keep a signed and dated record of the senior manager or delegate(s)' annual approval of the risk-based assessment methodology (RBAM), the list of Critical Assets (CAs) and the list of Critical Cyber Assets (CCAs), as required by CIP-002-2 R4. Texas RE_URE2 conducted a high-level review of a newly acquired station shortly after purchasing the station and registering with NERC. Texas RE_URE2 used a RBAM that applied to other assets from its fleet to identify CAs and CCAs within its new station, determined that it had no CAs and CCAs but failed to document its findings. This RBAM was used for four months until Texas RE_URE2 documented an updated RBAM for its newly acquired station, and used the RBAM to develop lists of CAs and CCAs. The RBAM, and lists of CAs and CCAs was approved by the senior manager or delegates four months after Texas RE_URE2 purchased the station and registered with NERC. Texas RE determined that the issue was from the date of Texas RE_URE2's registration with NERC to the date an updated RBAM and lists of CAs and CCAs were approved by the senior manager.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the issue was documentation in nature, as Texas RE_URE2 realized that it needed to update its RBAM, that it had no CAs or CCAs, but failed to update the RBAM and the existing list of CAs and CCAs and to keep a record of the senior manager's approval of these documents, as required. After applying the updated RBAM, Texas RE_URE2 determined that there were no CAs and CCAs at the facility at issue, and the senior manager or delegates approved the RBAM and the null lists of CCAs and CAs. Also, during the pendency of the issue, Texas RE_URE2 had a RBAM in place that was also applicable to other assets, performed a high-level review of this particular facility and correctly determined that it had no CAs or CCAs, thereby reducing the risk to the BPS to minimal.	Texas RE_URE2 updated the RBAM for the facility at issue and created a list of CAs and CCAs applying the updated RBAM. The list indicated that there were no CAs or CCAs at this facility. Texas RE_URE2's senior manager approved the RBAM and lists of CAs and CCAs. Texas RE verified completion of these mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2) CER-Quail Run Energy Partners LP (Quail Run)	NCRXXXXX	TRE201100534	CIP-003-2	R2	During a Spot-Check, Texas RE concluded that Texas RE_URE2 did not assign a single manager with overall responsibility and authority for leading and managing Texas RE_URE2's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2, as required by CIP-003-2 R2. Texas RE determined that when Texas RE_URE2 first registered with NERC, it properly assigned a single manager, as per CIP-003-2 R2. However another person, who was not the delegated single manager, approved Texas RE_URE2's updated risk-based assessment methodology (RBAM), the list of Critical Assets (CAs) and the list of Critical Cyber Assets (CCAs). Texas RE_URE2 realized the discrepancy and prepared documentation, stating that the person who approved the RBAM and the list of CAs and CCAs was in fact the proper, delegated manager and he had authority to approve these documents. Texas RE determined that because a different person, other than the initially authorized single manager, signed the RBAM and list of CAs and CCAs, Texas RE_URE2 was noncompliant with CIP-003-2 R2. Texas RE determined that the issue duration was a period of about three months.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Texas RE_URE2 had a senior manager with overall responsibility for compliance with CIP-002-2 through CIP-009-2 at all times. However, for the period of about three months the delegation of authority to a single senior manager with overall responsibility existed but was not documented. Texas RE determined that this issue was documentation in nature, thereby reducing the risk to the BPS to minimal.	Texas RE_URE2 documented the delegation of authority to a single senior manager. Texas RE verified completion of these mitigating 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)	Unidentified Registered Entity 3 (Texas RE_URE3)	NCRXXXXX	TRE2012010125	EOP-004-1	R3.1	Texas RE_URE3 submitted a Self-Report, stating that it experienced a reportable incident but it failed to provide a preliminary written report of the incident to its Regional Reliability Organization (Texas RE) and NERC within 24 hours of the incident, as required by EOP-004-1 R3.1. An inadvertent trip occurred to some of Texas RE_URE3's Units, removing over 1,000 MW of generation. As a result of these unit trips and combined loss of generation, system frequency dropped but ERCOT was able to restore the frequency level faster than the 15 minute system restoration requirement. Because Texas RE_URE3 experienced a trip of operating units that constituted a loss of over 1,000 MW of generation, the loss of generation was a reportable event, and Texas RE_URE3 had an obligation to submit a preliminary written report to its Regional Reliability Organization and to NERC within 24 hours, as required by EOP-004-1 R3. Texas RE_URE3 submitted a Preliminary Disturbance Report on the subject unit trip to Texas RE and NERC 10 days later. Since this time, all similar loss of generation events at Texas RE_URE3 have all been reported within 24 hours, as required.	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 risk was mitigated by several factors. First, Texas RE_URE3 notified its Reliability Coordinator (RC), ERCOT, of the trip via phone shortly after it occurred, and the RC timely submitted the same required information to Texas RE and NERC, as Texas RE_URE3 would have been submitted. Texas RE determined that the information submitted by Texas RE_URE3 10 days later was thus required, but redundant, because ERCOT already submitted the same information to Texas RE and NERC. Since this time, all similar loss of generation events at Texas RE_URE3 have all been reported within 24 hours, as required, as a result of the mitigating actions taken to mitigate this remediated issue. Finally, Texas RE did not find any reliability issues with this event and determined that this was a documentation issue.	Texas RE_URE3 submitted a Preliminary Disturbance Report on the subject unit trip to Texas RE and NERC as required by the Standard. In addition, Texas RE_URE3 verified that key personnel understand their reporting responsibilities. Texas RE verified completion of these mitigating activities.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012009697	CIP-006-3c	R5	WECC_URE1 submitted a Self-Report indicating an issue with CIP-006-3c R5. A WECC_URE1 employee accessed one of WECC_URE1's Physical Security Perimeters (PSP) to perform a business function. The PSP the employee accessed is a cabinet containing one Critical Cyber Asset (CCA) used for a WECC_URE1 management system. WECC_URE1's procedures for this PSP require a hard key to open the cabinet and a card must be swiped to turn off the events being monitored at the security center. WECC_URE1's procedures also require an employee to reactivate monitoring of the PSP after accessing the PSP by re-swiping their access card. In this case, after the employee involved was finished accessing the CCA, he failed to re-swipe the access card to reactivate monitoring of the PSP. The access system did not re-initiate monitoring of the cabinet until a security operator noticed that the cabinet was unmonitored. The security operator then force-armed the access system to once again begin monitoring the cabinet.	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 PSP in scope is locked using a hard key. In addition, the room containing the PSP is staffed with operational personnel twenty-four hours and electronic controls are in place for the one CCA. Finally, in case the CCA was compromised, the monitoring system frequency and unit output would have alerted the operational personnel.	This issue was remediated when monitoring was reactivated.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2) Southern California Edison - Transmission & Distribution Business Unit (SCET)	NCRXXXXX	WECC2012009390	CIP-006-3c	R1.6.2	WECC_URE2 self-certified noncompliance with CIP-006-3c R1.6.2. This Standard requires continuous escorted access of visitors within the Physical Security Perimeter (PSP). WECC determined that WECC_URE2 had an issue of CIP-006-3c R1.6.2 because three individuals requiring escorted access within a (PSP) had unescorted access for a period of approximately three minutes. The three individuals were unescorted in a WECC_URE2 PSP, which contained two Critical Cyber Assets (CCAs).	This issue did not pose a serious or substantial risk and only posed minimal risk to the reliability of the bulk power system (BPS) the three individuals only had physical access to the PSP. Also, the PSP is monitored twenty-four hours a day and each access point door is configured to generate an alarm for unauthorized access. In addition, the PSP is manned twenty-four hours a day.	This issue was remediated when the three individuals were escorted after the three minute issue duration.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) Pacific Gas and Electric Company (PGAE)	NCRXXXXX	WECC2012010272	CIP-002-3	R4	WECC_URE3 self-reported noncompliance with CIP-002-3 R4. According to the Self-Report, WECC_URE3 failed to annually approve the risk-based assessment methodology (RBAM), the Critical Asset list, and the Critical Cyber Asset (CCA) list for a calendar year. WECC_URE3 stated that it did perform an annual risk based assessment as required by CIP-002 before the end of the calendar year, the assigned CIP senior manager did not approve the documentation until after the required date. WECC reviewed WECC_URE2's Self-Report and its risk-based annual assessment. Specifically, WECC_URE3 performed its annual assessment of Critical Assets and CCAs prior to the end of the year and WECC_URE3 submitted its completed risk-based assessment and associated lists to the appropriate managers for approval. WECC_URE3's risk-based annual approval process is more robust than industry standard, in that it requires approval by two supplementary managers in addition to the assigned CIP senior manager. Based on WECC_URE3's document routing evidence, the annual approval process was initiated, reviewed, and approved by two WECC_URE3 managers, but not approved by the assigned CIP senior manager until 13 days late. This delay was a result of the CIP senior manager being out of the office for a holiday vacation.	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 WECC_URE3's annual assessment was initiated and completed except for the final approval of the CIP senior manager. The assessment was reviewed and approved by two of the three managers. The final approval was put on hold for 13 days until the assigned CIP senior manager returned from vacation. During the 13 days that the lists were not approved by the CIP senior manager, WECC_URE3's associated Critical Assets and CCAs were thoroughly identified, reviewed and approved by two WECC_URE3 managers that signed off on the assessment prior to the end of the year. Additionally, WECC_URE3 documentation had previously been annually approved in the year proceeding the noncompliant year and the year following the noncompliant year.	WECC_URE3's RBAM and updated Critical Asset and CCA lists were approved by the assigned CIP senior manager. WECC_URE3 moved its annual approval process to be performed earlier in the calendar to ensure the documentation is properly approved and recorded on an annual basis.

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)	NCRXXXXX	WECC2012010514	CIP-007-1	R4	WECC_URE4 self-reported an issue of CIP-007-1 R4. WECC reviewed WECC_URE4's Self-Report. According to the WECC, WECC_URE4 failed to use anti-virus and malware protection tools on sixty of its non-Cyber Asset and Critical Cyber Assets located within an Electronic Security Perimeter (ESP), but had not filed Technical Feasibility Exceptions (TFEs) for these devices. Although TFEs were not filed timely according to the requirement, WECC approved the TFEs pertaining to these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE4 submitted TFE Part A's for these devices which are in the "Accepted" status at WECC. As compensating measures, these devices reside in a Physical Security Perimeter PSP and ESP which are highly secured environments. These devices have no keyboards, CD/DVD drives, USB ports, or internet access, and the operating system is proprietary to the equipment so it has minimal exposure to viruses and malware.	WECC_URE4 remediated this issue when it submitted TFEs for the devices in scope.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2012010515	CIP-007-1	R5	WECC_URE4 self-reported an issue of CIP-007-1 R5. WECC reviewed the Self-Report and determined that WECC_URE4 failed to ensure that eight devices located within an Electronic Security Perimeter (ESP) require and use strong passwords, as required by CIP-007-1 R5.3. WECC_URE5 filed Technical Feasibility Exceptions (TFEs) for these devices late. WECC approved the TFEs pertaining to these devices.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because TFE Part A's for these devices were submitted and are in the "Accepted" status at WECC. WECC_URE4 stated that these devices reside in certain facilities and it is technically infeasible for these devices to have the protections of CIP-007-1 R5. As compensating measures these devices reside in a Physical Security Perimeter (PSP) and an ESP which are highly secured environments. These devices have no keyboards, CD/DVD drives, USB ports, or internet access, and the operating system is proprietary to the equipment so it has minimal exposure to viruses and malware.	WECC_URE4 remediated this issue when it submitted TFEs for the devices in scope.

Document Content(s)