Federal Energy Regulatory Commission
Washington, D.C. 20426
December 22, 2021

Re: FOIA No. FY19-30
Fortieth Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated November 30, 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. RC12-13, 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] The five-day notice period has elapsed and the document is enclosed.

Identities of Other Remaining UREs Contained Within RC12-13.

With respect to the remaining identities of UREs contained in RC12-13, 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

[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 staff initially determined that disclosure of identities may be appropriate.

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 RC12-13 will not be disclosed.

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

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

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2021.12.22 14:46:24 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC12-13

June 29, 2012

Southeastern Power Administration (SEPA)-.pdf page 35

City Of Gardner (Gardner)-.pdf page 36

Idaho Wind Partners 1, LLC (IWPL)-.pdf page 37

NorthWestern Corporation (NWC)-.pdf page 38

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 40 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 72 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 72 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 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 david.cook@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

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

cc: Entities listed in Attachment B

NERC

Attachment a

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

NERC

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR JUNE 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
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1731
dp.skaar@midwestreliability.org

Sara E. Patrick*
Director of Regulatory Affairs and Enforcement
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1708
se.patrick@midwestreliability.org

FOR NPCC:

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

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

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

FOR RFC:

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

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

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

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

FOR SERC:

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

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

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

FOR TEXAS RE:

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

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

FOR WECC:

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

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

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

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

NERC

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
June 29, 2012

Take notice that on June 29, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding forty (40) Registered Entities in eight (8) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Tatanka Wind Power, LLC (TWP)	NCR10245	MRO2012009979	FAC-008-1	R1	On October 28, 2011, TWP, as a Generator Owner (GO), self-certified noncompliance with FAC-008-1 R1 because it failed to document a Facility Ratings Methodology for developing Facility Ratings. TWP discovered this issue on June 27, 2011, when its parent company was developing a FAC-008-1 Facility Rating Methodology procedure to replace an existing Facility Rating procedure. TWP registered as a GO with MRO on April 29, 2008, and did not have a Facility Ratings Methodology until July 29, 2011.	MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although TWP did not have Facility Ratings Methodology, it did develop Facility Ratings. Additionally, TWP owns and operates a non-dispatchable interruptible wind generation resource, consisting of 120 1.5 MW wind turbine generators and is interconnected to a 230 kV transmission line. The interconnection facility owned and operated by TWP is designed to export the full aggregate capability of all 120 wind turbine generators while remaining below the normal rating of the equipment. TWP has not experienced any misoperations. Therefore, TWP's failure to document its Facility Ratings Methodology posed a minimal risk to the reliability of the BPS. Moreover, when rated per the new Facility Ratings Methodology, the changes to the TWP Facility Ratings were minimal.	TWP revised its Facility Rating Methodology on July 29, 2011. On May 29, 2012, MRO verified that TWP completed its mitigating activities on July 29, 2011.
Midwest Reliability Organization (MRO)	Tatanka Wind Power, LLC (TWP)	NCR10245	MRO2012009980	FAC-009-1	R1	On October 28, 2011, TWP, as a Generator Owner (GO), self-certified noncompliance with FAC-009-1 R1 because it failed to establish Facility Ratings consistent with its associated Facility Ratings Methodology. TWP discovered this issue on June 27, 2011, when its parent company was developing a FAC-008-1 Facility Rating Methodology procedure to replace an existing Facility Rating procedure. TWP registered as a GO with MRO on April 29, 2008, and did not have Facility Ratings consistent with its Facility Ratings Methodology until September 29, 2011.	MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although TWP did not have Facility Ratings Methodology, it did develop Facility Ratings. Additionally, TWP owns and operates a non-dispatchable interruptible wind generation resource, consisting of 120 1.5 MW wind turbine generators and is interconnected to a 230 kV transmission line. The interconnection facility owned and operated by TWP is designed to export the full aggregate capability of all 120 wind turbine generators while remaining below the normal rating of the equipment. TWP has not experienced any misoperations. Therefore, TWP's failure to document its Facility Ratings Methodology posed a minimal risk to the reliability of the BPS. Moreover, when rated per the new Facility Ratings Methodology, the changes to the TWP Facility Ratings were minimal.	TWP completed its Facility Rating Methodology on July 29, 2011 and has rated its facilities per the Methodology on September 29, 2011. On May 31, 2012, MRO verified that TWP completed its mitigating activities on September 29, 2011.
SERC Reliability Corporation (SERC)	Nashville Electric Service (NES)	NCR11077	SERC2012010004	FAC-009-1	R1	On April 4, 2012, NES, as a Transmission Owner, self-reported an issue with FAC-009-1 R1, stating it discovered Facility Ratings that were not in accordance with its Facility Rating Methodology (FRM) in three areas: (1) bushing current transformers (BCTs); (2) emergency conductor ratings; and (3) normal bus conductor ratings. SERC staff reviewed the NES 2010 Facility Ratings, which were in place when NES became a registered entity, and confirmed that NES had not properly accounted for secondary devices connected to BCTs when developing its Facility Ratings. In its Self-Report, NES stated that this error impacted the Normal Rating of seven transmission lines. SERC staff learned from NES engineers, however, that this error actually did not impact the overall Normal Ratings of any of its Facilities. SERC staff also confirmed that NES had not applied the correct operating temperature when calculating the emergency conductor ratings. The FRM states that the maximum operating temperatures for ACSR 795 conductors is 100º Celsius (C) for Normal Ratings and 140º C for Emergency Ratings. The 2010 Facility Ratings utilized 100º C for both Normal Ratings and Emergency Ratings. Based on the data NES provided, SERC staff concluded that the emergency conductor rating was not the Limiting Element when NES corrected this error. Finally, SERC staff confirmed that NES had not applied the correct operating temperature when calculating the normal bus conductor ratings. The FRM states that the maximum operating temperature under for substation rigid bus conductors was 90º C for Normal Ratings and 100º C for Emergency Ratings. The 2010 Facility Ratings utilized 100º C for both Normal Ratings and Emergency Ratings. Based on the data NES provided, SERC staff concluded that the bus conductor rating under Normal Ratings was not the Limiting Element when NES corrected this error. NES owns thirty-two 161 kV transmission lines and ten transformers. While none of NES's misapplications of its FRM affected the determination of the Limiting Element, the thirty-two transmission line Facility Ratings were not consistent with the NES FRM.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. NES's failure to properly apply its FRM for six months could cause equipment damage, incorrect modeling, and ultimately system outages; and 2. SERC staff found no evidence that NES's misapplications of its FRM affected its determination of the Limiting Element.	SERC staff verified that NES completed the following actions: 1. On March 28, 2011, NES reviewed and updated all Facility Ratings to include secondary devices, correct emergency conductor ratings, and correct substation bus conductor Normal Ratings; and 2. On April 4, 2012, NES revised its FRM to clarify the reference to rating secondary devices connected to BCTs.

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)	LG&E and KU Services Company as agent for Louisville Gas and Electric Company and Kentucky Utilities Company (LG&E & KU)	NCR01223	SERC2012009708	MOD-001-1a	R4	On February 10, 2012, LG&E & KU, as a Transmission Service Provider, self-reported an issue with MOD-001-1a R4, stating that a revised version of the Available Transfer Capability Implementation Document (ATCID) was made effective prior to notifying the parties specified in R4.1 through R4.6. SERC staff reviewed the revised ATCID as well as the email notification that was sent to the parties specified in R4.1 through R4.6. LG&E & KU's changes did not impact the Available Transfer Capability (ATC) methodology or how ATC is calculated. Rather, the changes were made to reflect changes within the organization and data distribution handling. Both the prior ATCID and revised ATCID stated that "[a]n ATCID update notification will be sent prior to the effective date of the update." The effective date for the revised ATCID was January 1, 2012. LG&E & KU sent an email notification to the necessary parties on January 3, 2012, the first business day following the effective date, and posted the new ATCID to the OASIS webpage the same day.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. LG&E & KU sent notification of the revision to the necessary parties on the first business day following the effective date of the new revision; and 2. LG&E & KU's revisions to the ATCID did not impact the actual ATC calculation.	SERC staff verified that LG&E & KU completed the following actions: 1. Developed a written process with a checklist that describes the future document control, posting, and notification requirements with respect to ATCID updates; 2. Developed training material covering the process and/or checklist governing document control, posting, and notification requirements with respect to ATCID updates; and 3. Trained appropriate Transmission Policy & Tariffs personnel to ensure a thorough understanding of the process and/or checklist that was developed to ensure proper document control, posting, and notification requirements of the ATCID.
SERC Reliability Corporation (SERC)	Ameren Services Company (Ameren)	NCR01175	SERC201000478	PRC-005-1	R2; R2.1	On February 9, 2010, Ameren, as a Transmission Owner (TO), self-reported an issue with PRC-005-1 R2.1, stating that nine Protective Relays were not tested within the intervals defined in Ameren's Protection System maintenance and testing program. On May 17, 2010, Ameren submitted two additional Self-Reports of issues with PRC-005-1 R2, both stating that Ameren had not performed maintenance on two Station Batteries (one battery per Self-Report). On January 26, 2011, Ameren self-reported an additional issues with PRC-005-1 R2, stating that it had not tested 31 Protective Relays within the intervals defined in Ameren's Protection System maintenance and testing program. SERC staff determined that these additional issues were related to the issues in the February 9, 2010 Self-Report, and involved the same Standard and requirement. SERC staff decided to review the incidents detailed in the May 17, 2010 and January 26, 2011 Self-Reports as an expansion of scope of the February 9, 2010 Self-Report. SERC staff reviewed a spreadsheet prepared by Ameren that included each of Ameren's TO Protection System devices and the defined maintenance and testing intervals, the most recent test date, and the previous test date for each device. SERC staff verified the assigned intervals based on a review of Ameren's PRC-005 maintenance and testing procedures. Based on this review, SERC staff determined that Ameren had 37 Protective Relays and two Station Batteries that were tested outside of the defined interval; and three Protective Relays with no test record of when the devices were last tested or maintained. In total, Ameren could not provide evidence that 42 out of 11,582 Protection System devices (or approximately 0.36%) were tested within the defined interval or had previous maintenance and testing records.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. Ameren tested all 40 relays and found them to be functional, suggesting the devices likely would have performed as intended if called upon to do so; 2. Ameren implements redundant protection schemes that would provide protection in the event that the relays failed; and 3. Ameren tested the two Station Batteries and found no problems, suggesting that the devices likely would have performed as intended if called upon to do so. In addition, the batteries were less than 10 years old and had alarms in place to notify operators of failure.	SERC staff verified that Ameren completed the following actions: 1. Assigned technicians to maintain the nine missed relays identified in the February 9, 2010 Self-Report; 2. Audited the entire Illinois transmission relay database to ensure that the 2010 calendar year schedule was comprehensive; 3. Enhanced the Ameren Protection System Maintenance and Testing Program (M&T Program) to augment the workflow process for determining the calendar year relay maintenance schedule with an independent database query and review; 4. Assigned personnel to maintain the battery identified in the first May 17, 2010 Self-Report and added the battery to Ameren's work management system so that future job requests for that battery will be issued quarterly and evidence of completion will be captured; 5. Reviewed Ameren's list of transmission substations and verified that the appropriate work group was assigned to maintain batteries pursuant to PRC-005 R1. 6. Developed and provided formal training for substation maintenance supervisors and engineers regarding transmission substation battery maintenance and documentation responsibilities pursuant to Ameren's M&T Program; 7. Upgraded the software for the transmission relay database to improve Ameren's ability to determine the interval between the last and previous test dates; and 8. Reviewed all Ameren Transmission Protection System devices to ensure they were compliant with Ameren's M&T Program.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	North Carolina Eastern Municipal Power Agency (NCEMPA)	NCR01284	SERC2011007962	PRC-008-0	R1	On August 26, 2011, NCEMPA, as a Distribution Provider, self-reported an issue with PRC-008-0 R1, stating that the Under Frequency Load Shedding (UFLS) program used by one of its members, the City of Washington, NC (City of Washington), did not include testing the underfrequency functionality. NCEMPA noted that it is registered as a JRO (JRO00085) on behalf of 15 municipalities, five of which, including the City of Washington, participate in Progress Energy Carolina's UFLS program. The municipalities participating in the UFLS program within NCEMPA have had UFLS equipment testing and maintenance programs, varying slightly between the municipalities, in place since June 18, 2007. NCEMPA believed that the respective UFLS programs were appropriate and adequate to fully comply with PRC-008 R1 and R2. On May 2, 2011, NCEMPA implemented a new UFLS equipment maintenance and testing program that consolidated and superseded the individual city programs. In preparation for an upcoming SERC Compliance Audit, NCEMPA hired a consultant to independently review all applicable standards. In August 2011, the consultant noted that the City of Washington's UFLS program may not have included testing of the underfrequency functionality. The City of Washington informed NCEMPA that while its UFLS equipment maintenance and testing program included functional relay testing for UFLS relays, the program did not provide for testing of the relays' underfrequency capability prior to the implementation of NCEMPA's UFLS equipment maintenance and testing program on May 2, 2011. SERC staff reviewed the City of Washington's UFLS equipment maintenance and testing procedure and confirmed that while the procedure contained a maintenance and testing schedule, the procedure did not contain an equipment list as required by R1. SERC staff confirmed with NCEMPA that the other four municipalities required to participate in the UFLS program had included an equipment list as required by R1 and were testing the underfrequency functionality of their UFLS equipment. NCEMPA has a total of 87 UFLS relays, nine of which were not identified in the City of Washington's equipment list in its UFLS equipment maintenance and testing procedure. Therefore, NCEMPA was missing UFLS equipment identification for 10.3% of its UFLS relays.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. NCEMPA was performing overcurrent trip and timing tests for the nine UFLS relays; 2. NCEMPA tested the underfrequency functionality of the nine UFLS relays and found that they were functioning properly; and 3. The City of Washington load shedding contribution is 21 MW (8% of the total NCEMPA underfrequency capability) and 0.17% of Progress Energy Carolina's 2011 annual peak load and would have minimal impact to the BPS.	SERC staff verified that NCEMPA completed the following actions: 1. On May 2, 2011, NCEMPA adopted the consolidated UFLS testing and maintenance program that applies uniformly to the five UFLS participating municipalities; 2. The consolidated program includes the list of NCEMPA equipment that participates in Progress Energy Carolina's UFLS program; 3. The consolidated program calls for a five year testing and maintenance interval for the UFLS equipment and specifically provides for testing and maintenance with respect to UFLS functionality. Pursuant to the new program, NCEMPA will have an independent contractor conduct UFLS testing and maintenance every five years; and 4. All relays owned by the five NCEMPA municipalities that participate in Progress Energy Carolina's UFLS program were tested and maintained during the first three months of 2011.
SERC Reliability Corporation (SERC)	Duke Energy Carolinas (Duke)	NCR01219	SERC201000628	VAR-001-1	R6	On September 28, 2010, Duke, as a Transmission Operator (TOP), self-reported an issue with VAR-001-1 R6, stating that it was not aware of the existence of power system stabilizers (PSSs) at eight units that were in service when the units were online and therefore would not know the status of the PSSs. While reviewing and updating documentation for VAR-001-1, Duke discovered that the six units at Rowan Combustion Turbines, an Independent Power Producer (IPP) within the Duke TOP footprint, had PSSs that were enabled when the units were online. Duke, as the TOP, was not aware of the existence of the PSSs on these six units, and therefore was not aware of their status. The generating units at Rowan are owned by the Southern Company and Duke does not operate them. After this discovery, Duke initiated a review to check all 211 generation units on the Duke system. Duke found two hydro units at its Keowee facility that had the PSSs enabled when the units were online. Duke, as the TOP, was not aware of the existence of the PSSs on these two units, and therefore was not aware of their status. The PSSs are configured to be enabled upon start up of the unit's automatic voltage regulator (AVR) and remain enabled during operation of the units. Because the PSS function is built in to the AVR, Duke did not have the ability to enable or disable this function. Duke stated that there was a lack of communication between internal groups which led to its lack of awareness of the existence of the PSSs for these two units. Once it identified all the affected units, Duke notified its system operators of the existence of the eight PSSs in the Duke footprint and their status. Duke, as a TOP, did not know the status of eight PSSs out of a total of 211 generating units on Duke's system, or approximately 3.8% of its transmission Reactive Power resources.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. No system or operation changes were required after identification of the PSSs. The presence or lack of a PSS on a unit requires no different treatment by Duke as a TOP because the PSS operation is fully automatic and requires no operator intervention; 2. The AVRs of the eight units can operate without the associated PSSs being in service; 3. The AVRs of the eight units were operating in automatic voltage control mode during the period of this issue; 3. Duke never changed the state of the two PSSs at the Keowee hydro units while synchronized to the BPS. In addition, the Keowee units rarely run, typically averaging about 5% capacity factor, and there is no set schedule for Keowee to run; and 4. The six IPP units run with the PSS in service as long as the AVR is on. The IPP plant runs with its AVR in service and controlling voltage and the Generator Operators (GOPs) have been instructed to notify Duke's System Operating Center if for any reason the AVR is turned off.	SERC staff verified that Duke completed the following actions: 1. Put a process in place between internal Duke groups to ensure appropriate operating personnel are made aware of future PSSs in service capability; 2. Conducted training for real-time operating personnel on the awareness of PSSs currently in service on the Duke system; 3. Disseminated correspondence to real-time operating personnel concerning the awareness of PSSs; 4. Sent a notification process for PSS status changes to GOPs and IPPs; 5. Disseminated internal correspondence to GOPs concerning the awareness of PSS requirements; 6. Enhanced the real-time electronic logging tool for the TOP to include a selection to document PSS status changes when notified by the GOP; 7. Upgraded AVR status page to include a PSS tab, which displays PSS status changes. 8. Updated system operations guide to incorporate the response process used by the TOP after notification of a PSS status change; and 9. Created a system operations reference document for training and for awareness of PSSs on the Duke system and their purpose.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Associated Electric Cooperative, Inc. (AECI)	NCR01177	SERC201100766	VAR-002-1	R1	On February 25, 2011, AECI, as a Generator Operator, self-reported an issue with VAR-002-1 R1, stating that it discovered that Units 10, 11, and 12 at its Chouteau plant were operating with the automatic voltage regulators (AVRs) in service controlling VARs but it could not confirm that AECI had notified the Transmission Operator (TOP) that it would operate those units in a mode other than automatic voltage control mode. In October 2010, as part of its compliance program, AECI sent a survey to each plant seeking verification that the generator units were operating with AVR in service and controlling voltage. All but one of the AECI operators responded affirmatively. The operator at AECI's Chouteau plant responded that Units 10, 11, and 12 were operating with AVR in service controlling VARs. SERC staff reviewed documentation provided by AECI but determined that none of the documentation demonstrated that AECI had notified the TOP prior to operating the three Chouteau generating units in a mode other than automatic voltage control mode.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. AECI maintained its voltage level within the bounds set by its TOP during the period of the issue; 2. AECI was able to respond to all changes that were required while in VAR control mode and could respond to Reliability Coordinator or TOP directives; and 3. This issue affected 629 MW of generation at the Chouteau plant, or approximately 12.0% of AECI's total capacity of 5,255 MW. At the time of the issue, the Chouteau plant was operating at a capacity factor of 37.5%.	SERC staff verified that AECI completed the following actions: 1. Immediately after discovering that three units at the Chouteau plant were operating in VAR control mode, AECI switched the units to automatic voltage control mode; and 2. The contractor operating the Chouteau plant for AECI revised its procedures to specify that the units must be operated in automatic voltage control mode.
SERC Reliability Corporation (SERC)	Associated Electric Cooperative, Inc. (AECI)	NCR01177	SERC2011008222	VAR-002-1	R1	On September 27, 2011, AECI, as a Generator Operator, self-reported an issue with VAR-002-1 R1, stating it had been operating three generation units at its Holden plant with the automatic voltage regulator (AVR) in service controlling VARs, not controlling voltage, and had not notified the Transmission Operator (TOP) that it would operate those units in a mode other than automatic voltage control mode. SERC staff learned that AECI requested a detailed refresher training class from the vendor on the vendor's control system for the Holden plant in September 2011. During training, AECI discovered that after the three Holden units started up and were running as expected, a signal was sent to the AVR after the generator breaker was closed, which switched the AVRs for these units from voltage control mode to VAR control mode. The operators at the Holden plant were unaware of this signal and the fact that the three units operated in VAR control mode after being connected to the grid, and therefore did not notify the TOP prior to operating the three units in a mode other than automatic voltage control mode.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. AECI maintained its voltage level within the bounds set by its TOP during the period of the issue ; 2. AECI was able to respond to all changes that were required while in VAR control mode and could respond to Reliability Coordinator or TOP directives; and 3. This issue affected 321 MW of generation at the Holden plant, or approximately 6.1% of AECI's total capacity of 5,255 MW. At the time of the issue , the Holden plant was operating at a capacity factor of 2%.	SERC staff verified that AECI completed the following actions: 1. AECI removed the control system logic that switched the Holden plant from voltage control mode to VAR control mode when the tie-breaker is closed. This change now allows the Holden plant to remain in voltage control mode after the units are connected to the grid; and 2. AECI investigated whether its other gas plants with similar control systems had a similar logic programmed into the control systems and found that only the Holden plant had this type of logic programmed into the control system.
SERC Reliability Corporation (SERC)	Settlers Trail Wind Farm LLC (STWF)	NCR11135	SERC2011008224	VAR-002-1.1b	R1	On September 28, 2011, STWF, as a Generator Operator, self-certified an issue with VAR-002-1.1b R1, stating that STWF was not yet in commercial operation and had not formally notified its Transmission Operator (TOP) until September 27, 2011 that its automatic voltage regulator (AVR) was not in automatic voltage control mode. SERC staff requested and reviewed additional information from STWF in order to complete its assessment. STWF stated that, due to the nature of all wind farms, STWF could not place its AVR in service until after a majority of the turbines were commissioned and turned over for operation. At the same time, each individual turbine cannot be commissioned without back feed power from the grid. STWF first put energy from the wind farm onto the grid during testing on June 2, 2011. SERC staff reviewed emails and operator logs demonstrating communications between STWF and its TOP, starting with the initial interconnection studies, through the design and construction process, and to commercial operation. These communications indicate that STWF's TOP was generally aware of the status of the STWF project, despite STWF's failure to notify the TOP that the AVR was not in automatic voltage control mode until September 27, 2011. On September 30, 2011, STWF notified its TOP that its AVR had been placed in service in automatic voltage control mode.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. STWF's TOP was aware that the STWF facility was in start-up operation and not yet in commercial operation; 2. Each wind turbine at the STWF facility operated independently during the test power stage and managed its own voltage and power factor during that time; and 3. STWF is a small-sized entity comprising 94 identical 1.6 MW wind generators with a combined capacity of 150 MW.	SERC staff verified that STWF completed the following actions: 1. Notified the TOP that the AVR was not in automatic voltage control mode on September 27, 2011; 2. Notified the TOP that the AVR had been placed in automatic voltage control mode on September 30, 2011; and 3. Developed a procedure to clarify the process for start-up and commissioning of the facility with respect to automatic voltage control, which will be provided to the TOP prior to energizing all new facilities.

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)	Settlers Trail Wind Farm LLC (STWF)	NCR11135	SERC2011008225	CIP-001-1a	R4	On September 28, 2011, STWF, as a Generator Operator (GOP), self-certified an issue with CIP-001-1a R4, stating that it had not established appropriate communications with local Federal Bureau of Investigation (FBI) officials. SERC staff requested and reviewed additional information from STWF in order to complete its assessment. SERC staff determined that STWF, located in Iroquois County, Illinois, initially used a sabotage reporting procedure that included local FBI contact information for Austin, Texas, where the dispatch center performing the GOP function is located. STWF did not use a sabotage reporting procedure that included local FBI contact information for Illinois until August 25, 2011, when it adopted a new procedure.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The procedure STWF used included FBI contact information for the dispatch center located in Austin, Texas, and the Texas FBI could have contacted the Illinois FBI if necessary; 2. STWF revised its procedure to include the Illinois FBI office on August 25, 2011, more than a month before STWF started commercial operation on October 1, 2011; and 3. STWF is a small-sized entity comprised of 94 identical 1.6 MW wind generators with a combined capacity of 150 MW.	SERC staff verified that STWF completed the following actions: Revised its sabotage reporting procedure to include local FBI contact information for Illinois. The updated contact information was a correct and working phone number at the referenced FBI office.
Southwest Power Pool Regional Entity (SPP RE)	American Electric Power Service Corp. As Agent For Public Svc. Co. Of Oklahoma & SW Ele Pwr Co. (AEPW)	NCR01056	SPP201000431	VAR-002-1.1a	R1	On October 6, 2010, AEPW self-reported a compliance issue with VAR-002-1.1a R1. AEPW's Stall power plant began commercial operation on June 16, 2010, and ran 48 days in manual Voltage and Reactive (VAR) power control mode instead of automatic voltage control mode without notifying the Transmission Operator (TOP), as required by VAR-002-1.1a R1. The start-up /commissioning personnel and plant operations did not initially recognize nor report that the automatic voltage regulator (AVR) was in manual VAR control mode instead of the required automatic voltage control mode and therefore AEWP failed to notify the TOP. This Standard applies to AEPW's Generator Operator (GOP) function.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although AEPW's AVRs were set in manual VAR control mode without notifying the TOP, AEPW monitored and maintained its voltage schedule during the period when its AVRs were in VAR control mode. Also, a power flow simulated study assuming AEPW's unit was providing no VAR support showed that no measurable change in system voltage would occur as a result of this issue. Finally, there were no operating events as a result of AEPW's failure to notify the TOP.	During the next applicable unit outage, AEPW changed the voltage regulators from VAR control mode to automatic voltage control mode after the initial relay and voltage regulator settings were changed. AEPW also surveyed its plant operations as a fleetwide evaluation of voltage regulator operating requirements, and communicated to the plant managers the requirement to maintain the AVR in service and in automatic voltage control mode unless they have notified the TOP. Finally, AEPW developed and implemented a training program for operation personnel to recognize voltage regulator operating and reporting requirements and a NERC compliance checklist to be completed prior to a plant commencing commercial operation to ensure new plants are configured properly and that staff are properly aware of NERC requirements before commercial operation. SPP RE verified that the mitigating activities were completed.
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100623	PRC-005-1	R1	During a June 8, 2011 through June 9, 2011 Compliance Audit, SPP RE discovered that Gardner had a compliance issue with PRC-005-1 R1 because Gardner did not have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the Bulk Electric System, as required by this Standard. SPP RE determined that the issue existed from when Gardner was required to comply with this Standard on December 20, 2007 to when Gardner mitigated the issue on January 1, 2010. This Standard applies to Gardner's Distribution Provider (DP) and Transmission Owner (TO) functions.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, Gardner's BPS facilities include one 161 kV substation (Substation 2) with two interconnections to Gardner's Transmission Operator (TOP), and several relays in an adjacent 161 kV substation that is owned and maintained by Gardner's TOP. Gardner's TOP was performing relay maintenance and testing of the Gardner electromechanical relays at the TOP's adjacent 161 kV substation, despite Gardner's lack of a PRC-005 maintenance and testing program. Second, Gardner demonstrated that it had performed testing of its microprocessor relays, communications systems, Direct Current (DC) circuitry, and batteries, in its Substation 2, prior to developing its PRC-005 maintenance and testing procedure. Although Gardner could not demonstrate that it had tested its voltage and current sensing devices in Substation 2 prior to 2010, Gardner would have become aware of any Potential Transformer (PT) or Current Transformer (CT) failures during its other relay testing activities because the microprocessor testing would have indicated the existence of failed PTs or CTs.	On January 1, 2010, Gardner implemented a Protection System maintenance and testing program, which addresses the requirements of PRC-005-1 R1. Gardner has committed to maintain and revise its Protection System maintenance and testing program as needed.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100624	PRC-005-1	R2	During a June 8, 2011 through June 9, 2011 Compliance Audit, SPP RE discovered that Gardner had a compliance issue with PRC-005-1 R2 because it did not provide evidence that its Protection System devices were maintained and tested within the defined intervals and the date each Protection System device was last tested/maintained. SPP RE determined that Gardner failed to perform (1) annual infrared testing on its Potential Transformers (PTs) or Current Transformers (CTs) in either 2008 or 2009; and (2) monthly battery tests prior to June 2011, as required by this Standard. Gardner failed to test 54 devices (63%) out of 86 total devices. SPP RE determined that the issue existed from when Gardner was required to comply with this Standard on December 20, 2007 to June, 2011, when Gardner performed monthly battery tests. This Standard applies to Gardner's Distribution Provider (DP) and Transmission Owner (TO) functions.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, Gardner's BPS facilities include one 161kV substation (Substation 2) with two interconnections to Gardner's Transmission Operator (TOP), and several relays in an adjacent 161 kV substation that is owned and maintained by Gardner's TOP. Second, although Gardner could not demonstrate that it had tested its voltage and current sensing devices in Substation 2 prior to 2010, Gardner would have become aware of any Potential Transformer (PT) or Current Transformer (CT) failures during its other relay testing activities because the microprocessor testing would have indicated the existence of failed PTs or CTs. Finally, although Gardner could not provide evidence of performing monthly battery tests prior to June 2011, Gardner was able to provide evidence demonstrating that it had performed an impedance test on its batteries within the intervals established in its Protection Systems maintenance and testing program.	Gardner developed a "Substation Monthly Checklist," to record the monthly battery inspections that are performed in accordance with its "PRC-005 Gardner Maintenance and Testing Procedure." Gardner also performed the annual CT and PT infrared testing for 2011 on November 10, 2011, and will continue to conduct testing in accordance with its "PRC-005 Gardner Maintenance and Testing Procedure."
Southwest Power Pool Regional Entity (SPP RE)	Red Hills Wind Project, LLC (RHWP)	NCR10304	SPP2011008457	FAC-008-1	R1	On October 28, 2011,RHWP, as a Generator Owner (GO), self-reported noncompliance with FAC-008-1 R1. RHWP stated that it did not have a documented Facility Rating Methodology (FRM) for developing Facility Ratings. SPP RE determined that the duration of this issue was from February 26, 2009, RHWP's effective NERC registration date, through July 29, 2011, when RHWP implemented a documented FRM.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although RHWP did not have a FRM, it did establish Facility Ratings. RHWP's facility was designed and constructed with its generators being the most limiting element . RHWP relied on original equipment manufacturing ratings, engineer design studies, and equipment test results to develop the Facility's Ratings. RHWP established a FRM on July 29, 2011 and rated its Facility per the newly established FRM on September 29, 2011. The results confirmed that RHWP's generators were the most limiting element, which was correctly identified before and after the establishment of the FRM.	On July 29, 2011, RHWP's parent company, Acciona Energy North America (AENA), completed the "AENA Standard FAC-008-1 Facility Rating Methodology" procedure for RHWP and conducted training of the relevant personnel. SPP RE verified that the mitigating activities were completed.
Southwest Power Pool Regional Entity (SPP RE)	Red Hills Wind Project, LLC (RHWP)	NCR10304	SPP2011008458	FAC-009-1	R1	On October 28, 2011, RHWP, as a Generator Owner (GO), self-reported noncompliance with FAC-009-1 R1. RHWP stated that it did not establish a Facility Rating for RHWP's Facility that was consistent with its associated Facility Ratings Methodology (FRM). The duration of this possible issue occurred from February 26, 2009, RHWP's effective NERC registration date, through September 29, 2011, the date on which RHWP rated its Facility using the associated FRM.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although RHWP did not have a Facility Rating established consistent with an associated FRM, it did establish Facility Ratings. RHWP's facility was designed and constructed with its generators being the most limiting element. RHWP relied on original equipment manufacturing ratings, engineer design studies, and equipment test results to develop the Facility Ratings. Following implementation of RHWP's FRM on July 29, 2011, RHWP rated its Facility and confirmed that the generators remained the most limiting element of the Facility.	On July 29, 2011, RHWP's parent company, Acciona Energy North America (AENA), completed the "AENA Standard FAC-008-1 Facility Rating Methodology" procedure for RHWP, and on September 29, 2011, RHWP rated its facility per its July 29, 2011 Methodology. The entity trained relevant personnel on the new FRM procedure. SPP RE verified that the mitigating activities were completed.
Southwest Power Pool Regional Entity (SPP RE)	Llano Estacado Wind, LP (Llano)	NCR10226	SPP201100659	PRC-005-1	R2.1	On August 1, 2011, Llano, as a Generator Owner (GO) self-reported a compliance issue with PRC-005-1 R2.1. Llano reported that subsequent to registering as a GO in March 3, 2008, it could not demonstrate that its Protection System devices were maintained and tested within the defined intervals, as required by this Standard. Llano failed to demonstrate that it conducted current annual battery tests in 2008 according to its Protection System maintenance and testing program. The batteries were the only components of Llano's Protection System devices that lacked an annual test in 2008 and all other components had been tested, and had documentation to confirm testing. SPP RE determined that this compliance issue was from March 3, 2008, when Llano was required to comply with this Standard, until May 2009.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by the following factors. First, although Llano could not demonstrate that it had current annual battery tests for 2008, it demonstrated that it was conducting regular, monthly battery inspections during this period of non-compliance, thereby reducing the risk to the BPS to minimal. Second, although Llano could not provide documented test results for 2008, Llano provided meeting minutes from a company meeting held on May 20, 2008, indicating that annual testing of its batteries was in fact conducted in 2008, as required by its Protection System maintenance and testing program. Finally, Llano's PRC-005-1 R1 Protection System maintenance and testing program addressed all five of its Protection System devices, including batteries.	Llano implemented a comprehensive maintenance scheduling and documentation tracking system to track contractor maintenance activities. Additionally, the maintenance requirements for Llano's PRC-005 equipment were loaded into its parent company's computerized maintenance monitoring system (CMMS). The CMMS is designed to notify the site operations staff of required maintenance activities. Also, site operations must sign off that maintenance has been completed and provide a copy of maintenance test results. If the maintenance is not completed, then an outstanding maintenance task remains open. The site operations staff has been trained on the Llano PRC-005 maintenance and testing program and on the corrective actions taken to ensure compliance with this Standard.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Westar Energy, Inc. (Westar)	NCR00658	SPP2012009698	PRC-018-1	R2	On February 15, 2012, Westar, as a Generator Owner (GO), self-reported noncompliance with PRC-018-1 R2. Westar discovered that it had not installed all required Disturbance Monitoring Equipment (DME) in accordance with the Regional Reliability Organization's installation requirements (Southwest Power Pool (SPP) Criteria 7.1.2) to facilitate analyses of events. Three Westar substations lacked Dynamic Disturbance Recorders (DDRs) capabilities although after the addition of interconnecting transmission lines, such DDRs capabilities were required by Criteria 7.1.2.	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). DDRs are important for event recording and historical event analysis but are not used in managing real-time system disturbances. Also, DDRs capabilities required by Criteria 7.1.2 are not essential for real-time operations, as evidenced by the fact that these requirements are waivable at SPP's discretion. Additionally, Westar did have other forms of disturbance monitoring capabilities at its three substations. Westar had installed Digital Fault Recorders (DFRs), Sequence of Events Recorders (SERs), and fault recording relays, which all aid in after-the-fact analysis of system events.	Westar conducted an extensive review to ensure DME equipment had been installed at all required locations and relevant personnel was trained on the new equipment. Additionally, Westar installed software in the DFRs at the three locations identified in the review, which allowed the devices to perform the functions of both a DFR and DDR. SPP RE verified that the mitigating activities were completed.
Western Electricity Coordinating Council (WECC)	Mission Valley Power (MVP)	NCR05241	WECC200810401	CIP-001-1	R4	MVP is subject to this Standard because it was registered on the NERC Compliance Registry on April 10, 2007 as a Load Serving Entity. On June 15, 2007, MVP filed a Self-Report addressing a possible issue of CIP-001-1 R4. MVP's sabotage response plan requires that its Power Dispatcher, as well as the appropriate parties in the Interconnection, must be notified of sabotage events affecting its system. MVP did not include FBI contact information in either the MVP sabotage response plan or its associated response checklist. Although this issue was self-reported prior to June 18, 2007, it became an enforceable post-June 18, 2007 possible issue when MVP did not complete the associated Mitigation Plan on the approved completion date. Enforcement reviewed the Self-Report, Mitigation Plan, and the Subject Matter Experts' findings and determined that MVP has a remediated issue of CIP-001-1 R4 because MVP's sabotage procedure and checklist did not contain the local FBI contact information as required.	WECC determined that this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. MVP has a process in place for reporting sabotage acts or events. Further, MVP did have a process in place for communication of information concerning sabotage events to appropriate parties in the Interconnection, however, MVP was missing a local FBI phone number.	MVP submitted its sabotage reporting procedures to WECC. MVP's sabotage reporting procedures included notification procedures including contact information for the local FBI. WECC verified MVP completed the actions outlined in the Mitigation Plan.
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801064	CIP-001-1	R1	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing a possible issue of CIP-001-1 R1 for its Load Serving Entity function. Specifically, NNSAL reported that it did not have formal procedures for disturbances or unusual occurrences, suspected or determined to be caused by sabotage. Particularly, NNSAL did not have formal procedures for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnections.	WECC determined that this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Although NNSAL did not have formal sabotage procedures consistent with CIP-001-1, it did have informal procedures in place that offset the risk posed by NNSAL's noncompliance. Specifically, NNSAL employees who noticed suspicious activities or conditions (which could be sabotage) would report the situation to the Los Alamos National Laboratory (LANL) Emergency Operations Center, which in turn would contact the appropriate law enforcement officials, including the FBI. Further, a resident FBI agent is located at the NNSAL Laboratory, which has direct contact with the FBI. Finally, The Department of Energy has a manual, DOE M 470.4-1 (August 26, 2005), "Safeguards and Security Program Planning and Management," which requires observation for and reporting of suspicious behavior that NNSAL informally adheres to. NNSAL had informal sabotage reporting procedures for the 11 months that it was creating formal procedures.	NNSAL created formal procedures and training for NNSAL operating personnel to make them aware of sabotage events on its facilities and for the communication of information concerning sabotage events to appropriate parties. WECC verified NNSAL completed the actions outlined in the Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801065	CIP-001-1	R2	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing a possible issue of CIP-001-1 R1 for its Load Serving Entity function. Specifically, NNSAL reported that it did not have formal procedures for the communication of information concerning sabotage events.	WECC determined that this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Although NNSAL did not have formal sabotage procedures consistent with CIP-001-1, it did have informal procedures in place that offset the risk posed by NNSAL's noncompliance. Specifically, NNSAL employees who noticed suspicious activities or conditions (which could be sabotage) would report the situation to the Los Alamos National Laboratory (LANL) Emergency Operations Center, which in turn would contact the appropriate law enforcement officials, including the FBI. Further, a resident FBI agent is located at the NNSAL Laboratory, which has direct contact with the FBI. Finally, The Department of Energy has a manual, DOE M 470.4-1 (August 26, 2005), "Safeguards and Security Program Planning and Management," which requires observation for and reporting of suspicious behavior that NNSAL informally adheres to. NNSAL had informal sabotage reporting procedures for the 11 months that it was creating formal procedures.	NNSAL documented procedures for the communication of information concerning sabotage events. NNSAL performed training on the new, documented procedure. WECC verified NNSAL completed the actions outlined in the Mitigation Plan.
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801066	CIP-001-1	R3	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing a possible issue of CIP-001-1 R1 for its Load Serving Entity function. Specifically, NNSAL reported that it did not have formal response guidelines for operating personnel.	WECC determined that this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Although NNSAL did not have formal sabotage procedures consistent with CIP-001-1, it did have informal procedures in place that offset the risk posed by NNSAL's noncompliance. Specifically, NNSAL employees who noticed suspicious activities or conditions (which could be sabotage) would report the situation to the Los Alamos National Laboratory (LANL) Emergency Operations Center, which in turn would contact the appropriate law enforcement officials, including the FBI. Further, a resident FBI agent is located at the NNSAL Laboratory, which has direct contact with the FBI. Finally, The Department of Energy has a manual, DOE M 470.4-1 (August 26, 2005), "Safeguards and Security Program Planning and Management," which requires observation for and reporting of suspicious behavior that NNSAL informally adheres to. NNSAL had informal sabotage reporting procedures for the 11 months that it was creating formal procedures.	NNSAL documented sabotage response guidelines, including personnel to contact for reporting disturbances due to sabotage events. NNSAL performed training on the new, documented procedure. WECC verified NNSAL completed the actions outlined in the Mitigation Plan.
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801067	CIP-001-1	R4	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing a possible issue of CIP-001-1 R1 for its Load Serving Entity function. Specifically, NNSAL reported that it did not have documented communications contacts with the local FBI office, nor did it have formal reporting procedures for providing information to the FBI with regard to sabotage events.	WECC determined that this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Although NNSAL did not have formal sabotage procedures consistent with CIP-001-1, it did have informal procedures in place that offset the risk posed by NNSAL's noncompliance. Specifically, NNSAL employees who noticed suspicious activities or conditions (which could be sabotage) would report the situation to the Los Alamos National Laboratory (LANL) Emergency Operations Center, which in turn would contact the appropriate law enforcement officials, including the FBI. Further, a resident FBI agent is located at the NNSAL Laboratory, which has direct contact with the FBI. Finally, The Department of Energy has a manual, DOE M 470.4-1 (August 26, 2005), "Safeguards and Security Program Planning and Management," which requires observation for and reporting of suspicious behavior that NNSAL informally adheres to. NNSAL had informal sabotage reporting procedures for the 11 months that it was creating formal procedures.	NNSAL established formal communication contacts with the FBI and formally documented the contact information in the sabotage reporting procedures. NNSAL performed training on the new, documented procedure. WECC verified NNSAL completed the actions outlined in the Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801248	COM-001-1	R1	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing noncompliance with COM-001-1 R1. WECC determined the following: Although NNSAL had adequate and reliable communication facilities, NNSAL did not maintain formal procedures or adequate documentation related to its use of its existing telecommunications facilities which it uses for exchanging Interconnection and operating information with the appropriate Reliability Coordinator, and Balancing Authority. NNSAL did not document how its telecommunications facilities were redundant and diversely routed as required by COM-001-1 R1. NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the bulk power system (BPS). If NNSAL lost all such telecommunications facilities, NNSAL did have procedures to ensure it maintained its power supply from its Balancing Authority, including operating procedures to maintain a reliable system until such time as a communication link could be established.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the BPS. NNSAL maintained redundant and diverse telecommunications facilities as follows: NNSAL's primary communications link is a commercial landline with NNSAL's Balancing Authority and the Reliability Coordinator. This link is backed up by battery powered cell phones and a battery operated microwave with an established communication link with NNSAL's Balancing Authority. Further, NNSAL has fax communications between its facilities and its Balancing Authority as a tertiary communication system. Thus, throughout the noncompliance period, NNSAL had redundant (i.e., primary and assorted back-up) communication systems including diverse communication tools (landline, cell, microwave, and fax). Finally, NNSAL does not distribute power other than into its own service area, thus reducing and compensating for risks associated with its lack of a formal procedure related to NNSAL's communication coordination. NNSAL does not have links to other Reliability Coordinators, Transmission Operators or Balancing Authorities other than its Balancing Authority. As described above, NNSAL uses its communication links for routine business, with such use acting as continuous testing of the communication links. In all instances, NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the BPS.	NNSAL submitted a completed Mitigation Plan and supporting evidence which included a document titled "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377." This document includes comprehensive information regarding NNSAL's telecommunications program's procedures, responsibilities, definitions and training. NNSAL also included comprehensive information regarding NNSAL's telecommunications program's guidelines to manage, alarm, test and/or actively monitor vital telecommunications facilities in the "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document. Similarly, in this document NNSAL included procedures for the coordination of telecommunications among its respective areas, and formalized its procedures associated with the means to coordinate telecommunications among its respective areas, including the ability to investigate and recommend solutions to telecommunications problems within its area and with other areas. Finally, "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" outlined specific written operation instructions to follow during the loss of telecommunications facilities. NNSAL updated "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document in such a manner as to demonstrate compliance with COM-001 R1, R2, R3 and R5.
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801249	COM-001-1	R2	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing noncompliance with COM-001-1 R2. WECC determined that NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the bulk power system (BPS). NNSAL did not have formalized procedures associated with such management, monitoring, and testing, and did not give explicit special attention to equipment not used for routine communications as required by the Standard COM-001-1 R2.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the BPS. NNSAL maintained redundant and diverse telecommunications facilities as follows: NNSAL's primary communications link is a commercial landline with NNSAL's Balancing Authority and the Reliability Coordinator. This link is backed up by battery powered cell phones and a battery operated microwave with an established communication link with NNSAL's Balancing Authority. Further, NNSAL has fax communications between its facilities and its Balancing Authority as a tertiary communication system. Thus, throughout the noncompliance period, NNSAL had redundant (i.e., primary and assorted back-up) communication systems including diverse communication tools (landline, cell, microwave, and fax). Finally, NNSAL does not distribute power other than into its own service area, thus reducing and compensating for risks associated with its lack of a formal procedure related to NNSAL's communication coordination. NNSAL does not have links to other Reliability Coordinators, Transmission Operators or Balancing Authorities other than its Balancing Authority. As described above, NNSAL uses its communication links for routine business, with such use acting as continuous testing of the communication links. In all instances, NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the BPS.	NNSAL submitted a completed Mitigation Plan and supporting evidence which included a document titled "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377." This document includes comprehensive information regarding NNSAL's telecommunications program's procedures, responsibilities, definitions and training. NNSAL also included comprehensive information regarding NNSAL's telecommunications program's guidelines to manage, alarm, test and/or actively monitor vital telecommunications facilities in the "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document. Similarly, in this document NNSAL included procedures for the coordination of telecommunications among its respective areas, and formalized its procedures associated with the means to coordinate telecommunications among its respective areas, including the ability to investigate and recommend solutions to telecommunications problems within its area and with other areas. Finally, "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" outlined specific written operation instructions to follow during the loss of telecommunications facilities. NNSAL updated "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document in such a manner as to demonstrate compliance with COM-001 R1, R2, R3 and R5.

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	WECC200801250	COM-001-1	R3	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing noncompliance with COM-001-1 R3. WECC determined that NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the bulk power system (BPS). NNSAL did not have formal alarming procedures for this equipment. NNSAL had the appropriate means to enable the reliable operation of its system and to enable and facilitate reliable operation of the BPS, but NNSAL could not demonstrate in a formal procedure how it provided a means to coordinate telecommunications among the respective areas around NNSAL's operations as required by COM-001-1 R3.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the BPS. NNSAL maintained redundant and diverse telecommunications facilities as follows: NNSAL's primary communications link is a commercial landline with NNSAL's Balancing Authority and the Reliability Coordinator. This link is backed up by battery powered cell phones and a battery operated microwave with an established communication link with NNSAL's Balancing Authority. Further, NNSAL has fax communications between its facilities and its Balancing Authority as a tertiary communication system. Thus, throughout the noncompliance period, NNSAL had redundant (i.e., primary and assorted back-up) communication systems including diverse communication tools (landline, cell, microwave, and fax). Finally, NNSAL does not distribute power other than into its own service area, thus reducing and compensating for risks associated with its lack of a formal procedure related to NNSAL's communication coordination. NNSAL does not have links to other Reliability Coordinators, Transmission Operators or Balancing Authorities other than its Balancing Authority. As described above, NNSAL uses its communication links for routine business, with such use acting as continuous testing of the communication links. In all instances, NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the BPS.	NNSAL submitted a completed Mitigation Plan and supporting evidence which included a document titled "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377." This document includes comprehensive information regarding NNSAL's telecommunications program's procedures, responsibilities, definitions and training. NNSAL also included comprehensive information regarding NNSAL's telecommunications program's guidelines to manage, alarm, test and/or actively monitor vital telecommunications facilities in the "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document. Similarly, in this document NNSAL included procedures for the coordination of telecommunications among its respective areas, and formalized its procedures associated with the means to coordinate telecommunications among its respective areas, including the ability to investigate and recommend solutions to telecommunications problems within its area and with other areas. Finally, "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" outlined specific written operation instructions to follow during the loss of telecommunications facilities. NNSAL updated "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document in such a manner as to demonstrate compliance with COM-001 R1, R2, R3 and R5.
Western Electricity Coordinating Council (WECC)	National Nuclear Security Administration - Los Alamos National Laboratory (NNSAL)	NCR05515	WECC200801252	COM-001-1	R5	On January 10, 2008, following an internal review of its Compliance Program, NNSAL submitted a Self-Certification addressing noncompliance with COM-001-1 R5. WECC determined that NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the bulk power system (BPS). Although NNSAL had formal operating procedures for its facility and informal communication procedures, NNSAL did not have a formalized NNSAL instructions and procedures to document how it would enable continued operation during the loss of telecommunications facilities as required by COM-001-1 R5. If NNSAL lost all such telecommunications facilities, NNSAL did have procedures to ensure it maintained its power supply from its Balancing Authority, including operating procedures to maintain a reliable system until such time as a communication link could be established.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the BPS. NNSAL maintained redundant and diverse telecommunications facilities as follows: NNSAL's primary communications link is a commercial landline with NNSAL's Balancing Authority and the Reliability Coordinator. This link is backed up by battery powered cell phones and a battery operated microwave with an established communication link with NNSAL's Balancing Authority. Further, NNSAL has fax communications between its facilities and its Balancing Authority as a tertiary communication system. Thus, throughout the noncompliance period, NNSAL had redundant (i.e., primary and assorted back-up) communication systems including diverse communication tools (landline, cell, microwave, and fax). Finally, NNSAL does not distribute power other than into its own service area, thus reducing and compensating for risks associated with its lack of a formal procedure related to NNSAL's communication coordination. NNSAL does not have links to other Reliability Coordinators, Transmission Operators or Balancing Authorities other than its Balancing Authority. As described above, NNSAL uses its communication links for routine business, with such use acting as continuous testing of the communication links. In all instances, NNSAL had the appropriate operating communications equipment to ensure reliable operation of its system and to enable and facilitate reliable operation of the BPS.	NNSAL submitted a completed Mitigation Plan and supporting evidence which included a document titled "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377." This document includes comprehensive information regarding NNSAL's telecommunications program's procedures, responsibilities, definitions and training. NNSAL also included comprehensive information regarding NNSAL's telecommunications program's guidelines to manage, alarm, test and/or actively monitor vital telecommunications facilities in the "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document. Similarly, in this document NNSAL included procedures for the coordination of telecommunications among its respective areas, and formalized its procedures associated with the means to coordinate telecommunications among its respective areas, including the ability to investigate and recommend solutions to telecommunications problems within its area and with other areas. Finally, "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" outlined specific written operation instructions to follow during the loss of telecommunications facilities. NNSAL updated "LANL Utilities and Infrastructure: Electric Operations Telecommunications 63-00-377" document in such a manner as to demonstrate compliance with COM-001 R1, R2, R3 and R5.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electric Coordinating Council (WECC)	Wood Group Power Operations (WGCS)	NCR10349	WECC2012009973	VAR-501-WECC-1	R1	WGCS's Panoche Energy Center is a peaking project under the control of the TOP (Pacific Gas and Electric (PG&E)) and it only operates when ordered by the Transmission Operator (TOP). On April 2, 2012, WGCS, as a Generator Operator, submitted a Self-Report for a possible issue of VAR-501-WECC-1 R1, based on the results of its quarterly Power System Stabilizer (PSS) report. On January 22, 2012, power from PG&E was lost. In order to save the batteries and control systems, WGCS shut down the generator controls. On January 23, 2012, power was restored to the plant. WGCS proceeded to activate the systems, which included powering up the controls used for operating the gas turbine/generator units, but it did not enable the PSS. WECC determined that when WGCS started up the system, the automatic voltage regulator (AVR) was operating in automatic voltage control mode, but the PSS's on the generator controls were not enabled. WGCS failed to ensure its PSS was in service 98% of all operating hours for synchronous generations equipped with PSS, in the first quarter of 2012.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. WGCS is a 400 MW simple-cycle power plant made up of four 100 MW gas turbine generating units. The PSS was in service between 90-95% of the time during the first quarter of 2012, and not the required 98% or greater. As a compensating measure, during the time the PSS was disabled, the AVR was still operating at 50 MW on all units. Therefore, the units would be able to respond to any system deviation. In addition, the WGCS units are not base load units, but a peaking facility dispatched by the TOP. Finally, the PSS was only offline for 14.75 hours for the first quarter of 2012.	WECC verified that WGCS has completed mitigating activities and this issue has been remediated. WGCS submitted a Mitigation Plan. WGCS completed the following activities to mitigate this issue: (1) added a PSS email alert to email all plan personnel plus the asset manager and regional project manager, whenever the PSS is disabled, (2) provided operator training to on the importance of verifying the AVR and PSS are enabled and functioning, and (3) created a quick reference reporting cord to add to the emergency operations book in the control room. WECC determined the duration of this issue was 14.75 hours, the length of time the PSS was off-line.
Western Electricity Coordinating Council (WECC)	Western Area Power Administration - Rocky Mountain Region (WACM)	NCR05464	WECC2012009730	TOP-007-WECC-1	R2	On February 28, 2012, WACM, as a Transmission Operator, self-reported potential noncompliance with TOP-007-WECC-1 R2. On two occasions, the Net Scheduled Interchange for power flow over major WECC path 21 (TOT2A) was over the path's System Operating Limit (SOL) when schedules for the next hour were implemented. The first instance occurred on September 20, 2011 during hour 22:00 that lasted from 11:01 PM to 11:39 PM, for a total of 38 minutes. During hour 22:00 the SOL for path TOT2A was 353 MW and the actual schedule values were 354 MW. The second instance occurred on path TOT2A on September 17, 2011 during hour 9:00 from 8:01 AM to 8:37 AM, for a total of 36 minutes. The SOL for TOT2A during this time was 353 MW and the actual schedule values were 354 MW. WECC determined that WACM was in noncompliance with TOP-WECC-007-1 R2 for scheduling power over a major WECC path when schedules for the next hour had been implemented.	The SOL for the major path was exceeded by less than an four percent for a limited duration of time. Accordingly, Enforcement determined that this posed a minimal risk to the reliability of the bulk power system.	WACM conducted training on the Standard to dispatchers that specifically addressed the standard and what the dispatchers should do to comply with it. Reviewed the events with the dispatchers and changed EMS to create audible and visual alarms to identify when there is a realtime sol exceedence.
Western Electricity Coordinating Council (WECC)	Idaho Power Company (IPCO)	NCR05191	WECC2012009308	VAR-002-1.1b	R1	IPCO, as a Generator Operator (GOP), conducted an internal assessment of VAR-002-1.1b and discovered one instance on October 14, 2010, where the Generation Dispatcher log did not document that the Transmission Operator (TOP) was notified when an Automatic Voltage Regulator (AVR) was off or in manual mode. IPCO's Generation Dispatcher sits in the same control room as the TOP. Typically, communication between the Generation Dispatcher and TOP concerning AVR status happens verbally and is then logged on the Generation Dispatcher's log. WECC determined that IPCO's Generator Operator (GOP) function operated a generator connected to the interconnected transmission system in other than the automatic voltage control mode without notifying the TOP, resulting in a possible noncompliance with VAR-002-1.1b R1.	IPCO does not have documentation to confirm that its Generator Operators notified the Transmission Operator when an AVR was off or in manual mode on one occasion and does not have documentation to confirm that the Generation Dispatcher verbally notified the TOP of a status or capability change of a PSS or AVR within the required 30. However, IPCO has numerous generating units at multiple facilities under its control, thus minimizing the impact of non-notification associated with an isolated change in status of a Power System Stabilizer (PSS) or AVR at any one unit. Further, the Generator Dispatchers reside in the same control room as the TOPs and IPCO's process includes verbal communication of generation outages and changes in status. For these reasons, WECC determined these issues posed minimal risk to the reliability of the bulk power system.	IPCO ensured its generator operated in the appropriate mode, notified the Transmission Operator, and developed procedures to minimize the likelihood of recurrence.
Western Electricity Coordinating Council (WECC)	Idaho Power Company (IPCO)	NCR05191	WECC2012009309	VAR-002-1.1b	R3	IPCO, as a Generator Operator (GOP), conducted an internal assessment of VAR-002-1.1b and discovered one instance on October 14, 2010, where the Generation Dispatcher log did not document that the Transmission Operator (TOP) was notified when an Automatic Voltage Regulator (AVR) was off or in manual mode. IPCO's Generation Dispatcher sits in the same control room as the TOP. Typically, communication between the Generation Dispatcher and TOP concerning AVR status happens verbally and is then logged on the Generation Dispatcher's log. WECC determined that IPCO's Generator Operator (GOP) function operated a generator connected to the interconnected transmission system in other than the automatic voltage control mode without notifying the TOP, resulting in noncompliance with VAR-002-1.1b R1. Additionally, IPCO's documentation did not indicate the expected duration of the change in status or capability nor could the IPCO assessment team determine in most cases whether the (verbal) notification occurred within 30 minutes of the status change. Thus, WECC determined IPCO was in noncompliance with VAR-002-1.1b R3 for failing to notify the associated Transmission Operator as soon as practical, but within 30 minutes of a status or capability change of each automatic voltage regulator and power system stabilizer and the expected duration of the change in status or capability.	IPCO does not have documentation to confirm that its Generator Operators notified the Transmission Operator when an AVR was off or in manual mode on one occasion and does not have documentation to confirm that the Generation Dispatcher verbally notified the TOP of a status or capability change of a PSS or AVR within the required 30. However, IPCO has numerous generating units at multiple facilities under its control, thus minimizing the impact of non-notification associated with an isolated change in status of a Power System Stabilizer (PSS) or AVR at any one unit. Further, the Generator Dispatchers reside in the same control room as the TOPs and IPCO's process includes verbal communication of generation outages and changes in status. For these reasons, WECC determined these issues posed minimal risk to the reliability of the bulk power system.	IPCO ensured its generator operated in the appropriate mode, notified the Transmission Operator, and developed procedures to minimize the likelihood of recurrence.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100437	CIP-003-3	R6	FRCC_URE1 self-reported that on one occasion, it implemented a change without documenting approval of the appropriate system control owner or manager, as required by FRCC_URE1's change control and configuration management procedure, which resulted in an issue with CIP-003-3 R6.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Even though the approval of the change was not documented prior to the change, verbal approval was acquired prior to implementation and all the Cyber Assets were tested pursuant to the requirements of CIP-007 R1 for any adverse effects to the existing cyber security control.	FRCC_URE1 completed mitigation activities by conducting an incident review with the FRCC_URE1 personnel responsible for compliance with the Standard and a review of the change management procedure with the energy management system team responsible for implementing the change.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007514	CIP-002-3	R2	During a FRCC CIP Compliance Audit, it was determined that FRCC_URE1 failed to correctly apply its risk-based assessment methodology as required by CIP-002-3 R1. FRCC_URE1 failed to identify as Critical Assets all transmission facilities at a single station or substation location that are identified by the Reliability Coordinator (RC), Planning Authority, or Transmission Planner as critical to the derivation of Interconnection Reliability Operating Limits (IROLs) and their associated contingencies. Specifically, FRCC_URE1 failed to include one facility that was identified by its RC as an IROL derivative asset, resulting in an issue with CIP-002-3 R2. Thus, FRCC_URE1's Critical Asset list was incomplete for a period of less than 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 even though the asset was a Critical Asset, it had been determined in previous years' assessments that FRCC_URE1 had no Critical Cyber Assets. All the Cyber Assets at the identified Critical Asset used non-routable protocol (serial only) and hence no CIP Standards were applicable.	FRCC_URE1 completed mitigation activities by updating the Critical Asset list and Critical Cyber Asset list. The addition of the new Critical Asset did not result in any new Critical Cyber Assets.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007521	CIP-007-2a	R7	During a FRCC CIP Compliance Audit, it was determined that FRCC_URE1 failed to demonstrate that prior to redeployment of its dispatch training workstations, FRCC_URE1 erased the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data. FRCC_URE1 redeployed the Cyber Assets outside the Electronic Security Perimeter (ESP) without ensuring that the data storage media were erased.	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 most of the cyber security-related information and data was erased from the system using the multiple pass erase method. Additionally, systems were removed from the ESP but were protected by the same Physical Security Perimeter (PSP) and with identical access protection as that employed for Critical Cyber Assets (CCAs). Since these systems were not critical to reliable operation, they were deployed outside the ESP and still controlled and operated by the FRCC_URE1 control center staff.	FRCC_URE1 completed mitigation activities by reviewing the configuration of the assets that were redeployed and confirmed that no CCA-related information exists. FRCC_URE1 has also updated its procedure for allowing exceptions to the cyber security policy.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007522	CIP-009-1	R4	During a FRCC CIP Compliance Audit, it was determined that FRCC_URE1 failed to demonstrate that its recovery plans included processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. There were no processes and procedures available that demonstrated the backup and storage of information for energy management system workstations, network switches and firewalls.	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 FRCC_URE1 did not document the location or process for storage and retrieval of the backup data, FRCC_URE1 provided sufficient evidence to demonstrate that all the required data was backed up for use in restoration.	FRCC_URE1 completed mitigation activities by documenting steps for backing up the data required for restoration.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100378	CIP-006-1	R1; R1.1	During a Spot Check, MRO discovered that MRO_URE1 failed to establish a six-wall boundary for a server cabinet in a supervisory control and data acquisition room. The server cabinet resides within an identified Physical Security Perimeter (PSP), but it did not have a completely enclosed border and no alternative measures were documented. Specifically, the server cabinet did not have a solid bottom and it was not secured to the floor, failing to meet the six-wall criteria. The space between the cage door and the floor beneath the floor tile was at least 12 inches by 24 inches or 288 square inches.	MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the server cabinet was not bolted to the floor, creating a six-walled boundary, it was within an identified PSP. The cabinet was located within a secure room itself, it just needed to be bolted to the floor.	Upon discovery of the issue, the cabinet was bolted to the floor and the work was completed prior to audit staff departure from MRO_URE1. MRO verified that MRO_URE1 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100379	CIP-006-1	R3	During a Spot Check, MRO discovered that MRO_URE1 failed to document and implement technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter (PSP) twenty-four hours a day, seven days a week. Specifically, MRO_URE1 failed to monitor two access points. A security cabinet utilized to secure the physical access control system has two side panels that are hard key accessible, and both access points were not monitored.	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 physical access points in question were sealed access doors to equipment cabinets, within a secure perimeter. The access doors can only be opened with a key, which was destroyed by MRO_URE1 upon installation. In addition, the cabinet is within a restricted area accessible only by key cards and by personnel with proper CIP privileges, such as individuals with personnel risk assessments and relevant training.	MRO_URE1 implemented an alert system to detect unauthorized access through the security cabinet panels. MRO verified that MRO_URE1 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100380	CIP-006-1	R4	MRO discovered that MRO_URE1 failed to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter (PSP). Specifically, MRO_URE1 failed to monitor two access points. A security cabinet utilized to secure the physical access control system has two side panels that are hard key accessible, and both access points were not monitored or logged.	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 physical access points in question were sealed access doors to equipment cabinets, within a secure perimeter. The access doors can only be opened with a key, which was destroyed by MRO_URE1 upon installation. In addition, the cabinet is within a restricted area accessible only by key cards and by personnel with proper CIP privileges, such as individuals with personnel risk assessments and relevant training.	MRO_URE1 implemented manual logging and installed signage at the side panel to ensure log entries are made. For cases where someone may gain unauthorized access through a panel, an alert system was implemented. MRO verified that MRO_URE1 completed its mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100374	CIP-007-3	R3; R3.1	MRO_URE2 self-reported noncompliance with CIP-007-3 R3 because it failed to review and document one security patch within thirty days. MRO_URE2 discovered that a security patch assessment had not been completed for one device for a three-month period. Although the vendor failed to notify MRO_URE2 that the security patch had been released, further investigation revealed that a patch had been released by the vendor in the previous year. Upon discovery, the patch was assessed and determined to be "not applicable" to the device.	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. MRO_URE2 has an account management system which restricts access to the device. Additionally, the single patch that was missed for the vendor device was a non-security patch that was not applicable to MRO_URE2's device type and configuration, and therefore did not require installation.	MRO_URE2 assessed the patch release with existing security patches for applicability. No installations were necessary because the patch was not applicable to MRO_URE2's systems. MRO verified that MRO_URE2 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO2012009747	CIP-004-3	R4; R4.1	MRO_URE2 self-reported noncompliance with CIP-004-3 R4 because it failed to revoke physical access within seven calendar days for an intern who no longer required such access to Critical Cyber Assets. The intern's business need for the physical access to two locations ended. The intern's supervisor did not report to the same physical location as the intern, so the end of business need was not immediately visible to the supervisor. In advance of his termination, the intern's physical access to one of the two locations was removed by a local and informal supervisor. The other access type was not included in that request. The intern's supervisor was on vacation at the time the business need ended, and did not immediately enter the termination or contact the help desk directly to have the intern's access removed. The following month, the supervisor returned from vacation and removed access.	MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the security access was not revoked from the intern's badge, the intern left his badge at the security desk on his last day of work. Additionally, everyone at the facility was aware that the intern had returned to school and was no longer working. Also, the intern did not have cyber access privileges, and the physical access was removed 19 days after the individual's last day. Therefore, MRO_URE2 was 12 days late in removing the physical access for one location. Additionally, the individual did not use his physical access rights to the location after his need had expired.	MRO_URE2 removed access rights to the individual. MRO_URE2 initiated an access management internal audit in order to understand if more occurrences existed or if any process changes were necessary. At the completion of the internal audit, the NERC CIP team sent a letter and quick reference card to all MRO_URE2 NERC CIP supervisors and updated program documentation to send a letter and quick reference card to supervisors new to NERC CIP responsibilities at the time of their assignment to the area or group. MRO verified that MRO_URE2 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100384	CIP-006-1	R1; R1.1	During a Spot Check, MRO discovered that MRO_URE2 failed to establish a six-wall boundary for a server cabinet in a supervisory control and data acquisition room. The server cabinet resides within an identified Physical Security Perimeter (PSP), but it did not have a completely enclosed border and no alternative measures were documented. Specifically, the server cabinet did not have a solid bottom and it was not secured to the floor, failing to meet the six-wall criteria. The space between the cage door and the floor beneath the floor tile was at least 12 inches by 24 inches or 288 square inches.	MRO determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Although the server cabinet was not bolted to the floor, creating a six-walled boundary, it was within an identified PSP. The cabinet was located within a secure room itself, it just needed to be bolted to the floor.	Upon discovery of the issue, the cabinet was bolted to the floor and the work was completed prior to audit staff departure from MRO_URE2. MRO verified that MRO_URE2 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100385	CIP-006-1	R3; R3.1	During a Spot Check, MRO discovered that MRO_URE2 failed to document and implement technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter (PSP) twenty-four hours a day, seven days a week. Specifically, MRO_URE2 failed to monitor two access points. A security cabinet utilized to secure the physical access control system has two side panels that are hard key accessible, and both access points were not monitored.	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 physical access points in question were sealed access doors to equipment cabinets, within a secure perimeter. The access doors can only be opened with a key, which was destroyed by MRO_URE2 upon installation. In addition, the cabinet is within a restricted area accessible only by key cards and by personnel with proper CIP privileges, such as individuals with personnel risk assessments and relevant training.	MRO_URE2 implemented manual logging and installed signage at the side panel to ensure log entries are made. For cases where someone may gain unauthorized access through a panel, an alert system was implemented. MRO verified that MRO_URE2 completed its mitigation activities.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100386	CIP-006-1	R4; R4.1	During a Spot Check, MRO discovered that MRO_URE2 failed to implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter (PSP). Specifically, MRO_URE2 failed to monitor two access points. A security cabinet utilized to secure the physical access control system has two side panels that are hard key accessible, and both access points were not monitored or logged.	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 physical access points in question were sealed access doors to equipment cabinets, within a secure perimeter. The access doors can only be opened with a key, which was destroyed by MRO_URE2 upon installation. In addition, the cabinet is within a restricted area accessible only by key cards and by personnel with proper CIP privileges, such as individuals with personnel risk assessments and relevant training.	MRO_URE2 implemented manual logging and installed signage at the side panel to ensure log entries are made. For cases where someone gains unauthorized access through the panel, an alert system was implemented. MRO verified that MRO_URE2 completed its mitigation activities on.

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 2 (MRO_URE2)	NCRXXXXX	MRO201100387	CIP-004-3	R4; R4.1	MRO_URE2 self-reported noncompliance with CIP-004-3 R4 because it failed to ensure access lists for contractors and service vendors are properly maintained. A request was submitted to the help desk to get access for an individual vendor. The ticket was submitted as an incident management ticket, instead of an access change ticket. The help desk routed the incident management ticket (which lacks steward approval, personnel risk assessment (PRA) verification, and cybersecurity training verification) for access configuration. The request was completed and physical access was configured to a NERC CIP location without documented approval by the designated steward for the area. The individual already met the PRA and training prerequisites, so when the lack of documented steward approval in the correct module was discovered within three calendar days, the correct ticket was submitted and the approval was documented. Additionally, an access request was submitted for another individual for unescorted physical access. The request was approved by the supervisor the same day and by the steward three days later; however, a security guard added the clearance code to the badge of a different individual with the same name. During the quarterly access review, MRO_URE2 discovered the inconsistency and access was revoked for the inappropriate individual. Therefore, the individual had unauthorized access for eight days.	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 first issue dealt with an internal routing error giving access to an individual with approval by the wrong manager. The individual already had the appropriate PRA and CIP training, and was properly approved three days after the access was granted. The second issue dealt with giving incorrect access to an individual because he had the same name as another employee. Procedurally, MRO_URE2 always required verification of employee identification numbers before adding or removing access, the issue was caused by an error in following procedure. The individual only had access for eight days. This was an isolated incident and the personnel followed procedure otherwise. Additionally, the individual was part of the CIP program, with an updated PRA and CIP training for access to other areas, although not approved for this subject restricted area. The individual was improperly given access to the to a station which is over 100 miles from the individual's job locale. This issue was discovered during a quarterly review and fixed. MRO_URE2 verified that the improper individual never actually accessed the area for which he was erroneously granted access.	When the lack of documented steward approval was discovered, a formal request was submitted to obtain that specific approval. Immediately upon discovery of the incorrect individual approval on the reports for authorized/actual access, the wrong individual's access was removed. The correct individual received access on his badge to the correct location. The guards have been retrained and the dual verification form updated to include an employee identification number column. The guards are now required to document the employee identification number of the person for which they are adding or removing access. Procedurally, the guards were always required to and are still required to verify the employee identification number before adding or removing access; however, now it is documented on the dual verification form. An updated form was implemented. MRO verified that MRO_URE2 completed its mitigating activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009039	CIP-006-3a	R2.2	During a NPCC CIP Compliance Audit, it was determined that NPCC_URE1 had an issue with CIP-006-3c R2.2. NPCC determined that NPCC_URE1 failed to timely perform a cyber vulnerability assessment for the servers that are involved with the physical access control system (PACS), as specified in CIP-007-3 R8. The cyber vulnerability assessment for the servers at issue was performed approximately six months late. NPCC_URE1's parent company performs vulnerability assessments on a corporate level. Failure to complete the vulnerability assessment, as described above, affected multiple registered entities, including NPCC_URE1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the servers at issue are not used to monitor or control BPS assets. They control the card-reader system that is utilized to control the Physical Security Perimeter's (PSP) physical access points. In addition to the card-reader system, NPCC_URE1 utilizes security guards and video cameras to monitor access to the PSP. NPCC_URE1 also has strict controls in place for providing physical access to Critical Cyber Assets. NPCC took into account that NPCC_URE1 had previous violations of this Standard. NPCC determined that the instant facts and circumstances were distinguishable and did not represent recurring conduct. None of the prior violations involved cyber vulnerability assessments. Rather, the prior violations involved improper methods of accessing the PSP. Specifically, each of the prior violations involved personnel using a key, as opposed to a card key, to access the PSP. These individuals had been issued keys prior to the effective date of the Reliability Standards, but were not issued card keys for unescorted access to Critical Cyber Assets. In order to mitigate these violations, NPCC_URE1 installed devices that disable the key locks except to allow access by authorized individuals only at a time when the key card reader unit is inoperable. The keys to these new lock devices were issued only to authorized personnel and are used only during emergencies when the key card reader is inoperable. Because the instant issue involved a cyber vulnerability assessment which was performed late, NPCC determined that the issue did not represent recurring conduct by NPCC_URE1.	NPCC_URE1 completed the vulnerability assessment for the servers at issue and revised its compliance assessment process document.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008448	CIP-006-3a	R2.2	NPCC_URE2 self-reported an issue with CIP-006-3a R2.2. During a NPCC CIP Compliance Audit, it was determined that NPCC_URE2 failed to timely perform a cyber vulnerability assessment for the servers that are involved with the physical access control system (PACS), as specified in CIP-007-3 R8. The cyber vulnerability assessment for the servers at issue was performed approximately six months late. NPCC_URE2 performs vulnerability assessments on a corporate level. Failure to complete the vulnerability assessment, as described above, affected multiple registered entities.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the servers at issue are not used to monitor or control BPS assets. They control the card-reader system that is utilized to control the Physical Security Perimeter's (PSP) physical access points. In addition to the card-reader system, NPCC_URE2 utilizes security guards and video cameras to monitor access to the PSP locations. NPCC_URE2 also has strict controls in place for providing physical access to Critical Cyber Assets.	NPCC_URE2 completed the vulnerability assessment for the servers at issue and revised its compliance assessment process document.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008447	CIP-006-3a	R2.2	NPCC_URE3 self-reported an issue with CIP-006-3a R2.2. During a NPCC CIP Compliance Audit, it was determined that NPCC_URE3 failed to timely perform a cyber vulnerability assessment for the servers that are involved with the physical access control system (PACS), as specified in CIP-007-3 R8. The cyber vulnerability assessment for the servers at issue was performed approximately six months late. NPCC_URE3's parent company performs vulnerability assessments on a corporate level. Failure to complete the vulnerability assessment, as described above, affected multiple registered entities, including NPCC_URE3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the servers at issue are not used to monitor or control BPS assets. They control the card-reader system that is utilized to control the Physical Security Perimeter's (PSP) physical access points. In addition to the card-reader system, NPCC_URE3 utilizes security guards and video cameras to monitor access to the PSP. NPCC_URE3 also has strict controls in place for providing physical access to Critical Cyber Assets.	NPCC_URE3 completed the vulnerability assessment for the servers at issue and revised its compliance assessment process document.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011009018	CIP-007-3	R5; R5.1; R5.1.2; R5.3	NPCC_URE4 self-certified that there was an issue with the credentials window associated with a radio-frequency identification (RFID) system on certain terminals that can access the energy management system in NPCC_URE4's control room and backup control center. It was observed that if a user disregarded the credentials window, he or she could manipulate the other windows populating the desktop behind the credentials window. NPCC determined that NPCC_URE4 had an issue with CIP-007-3 R5.1 and R5.3, since effective controls were not in place for authentication and accountability for access and user activity.	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 only control room personnel had access to the console on which the RFID readers were enabled. In addition, this system was used only for operator training, in a training room environment intended to simulate all aspects of the real-time systems. However, this training environment is on a separate network and completely isolated from the Electronic Security Perimeter (ESP).	NPCC_URE4 disabled the badge reader on systems not individually manned 24/7 and required users to enter a valid user name and password. This action was undertaken at both NPCC_URE4's control room and backup control center. The system manufacturer sent a corrective patch and a supervisor tested the installation and verified that the patch did resolve the issue. All terminals using the RFID system have been patched and have been verified to be working as designed.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100792	CIP-007-1	R5.2.3	RFC_URE1 self-reported an issue with CIP-007-1 R5.2.3 to Reliability*First*. RFC_URE1 discovered that it failed to maintain an audit trail of the account use for multiple shared accounts on its transmission management system and shared accounts in the substation network. Although there was a policy in place to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts, the program which runs the automated audit trails malfunctioned so the automated audit trails failed to function in this instance.	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 individuals who had access to the shared accounts during the relevant time period were properly authorized, had completed training, and had current personnel risk assessments. In addition, RFC_URE1 experienced no cybersecurity incidents during the relevant time period.	RFC_URE1 established manual audit trails for shared accounts on the substation networks and the transmission management system networks. RFC_URE1 tracked and reviewed these audit trails.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100802	CIP-007-1	R5.2.3	RFC_URE2 self-reported an issue with CIP-007-1 R5.2.3 to Reliability*First*. RFC_URE2 discovered that it failed to maintain an audit trail of the account use for multiple shared accounts on its transmission management system and shared accounts in the substation network. Although there was a policy in place to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts, the program which runs the automated audit trails malfunctioned so the automated audit trails failed to function in this instance.	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 individuals who had access to the shared accounts during the relevant time period were properly authorized, had completed training, and had current personnel risk assessments. In addition, RFC_URE2 experienced no cybersecurity incidents during the relevant time period.	RFC_URE2 established manual audit trails for shared accounts on the substation networks and the transmission management system networks. RFC_URE2 tracked and reviewed these audit trails.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100811	CIP-007-1	R5.2.3	RFC_URE3 self-reported an issue with CIP-007-1 R5.2.3 to Reliability*First*. RFC_URE3 discovered that it failed to maintain an audit trail of the account use for multiple shared accounts on its transmission management system and shared accounts in the substation network. Although there was a policy in place to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts, the program which runs the automated audit trails malfunctioned so the automated audit trails failed to function in this instance.	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 individuals who had access to the shared accounts during the relevant time period were properly authorized, had completed training, and had current personnel risk assessments. In addition, RFC_URE3 experienced no cybersecurity incidents during the relevant time period.	RFC_URE3 established manual audit trails for shared accounts on the substation networks and the transmission management system networks. RFC_URE3 tracked and reviewed these audit trails.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100793	CIP-007-1	R6.5	RFC_URE1 self-reported an issue with CIP-007-1 R6.5 to Reliability*First*. RFC_URE1 maintained logs of system events related to cybersecurity but had no documentation to verify that it reviewed the security logs from its transmission management system.	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. RFC_URE1 protects the transmission management system with layers of defenses beginning with physical security access controls that isolate the hosts from unauthorized access and any potential vulnerabilities. In addition, RFC_URE1's parent company corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections constitute a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to RFC_URE1's transmission management system. In addition, although RFC_URE1 failed to review the security logs, the security logs for the transmission management system did exist. When RFC_URE1 subsequently reviewed these logs, it found no threatening anomalies.	RFC_URE1 implemented manual monthly security log reviews.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100803	CIP-007-1	R6.5	RFC_URE2 self-reported an issue with CIP-007-1 R6.5 to Reliability*First.* RFC_URE2 maintained logs of system events related to cybersecurity had no documentation to verify that it reviewed the security logs from its transmission management system.	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. RFC_URE2 protects the transmission management system with layers of defenses beginning with physical security access controls that isolate the hosts from unauthorized access and any potential vulnerabilities. In addition, RFC_URE2's parent company corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections constitute a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to RFC_URE2's transmission management system. In addition, although RFC_URE2 failed to review the security logs, the security logs for the transmission management system did exist. When RFC_URE2 subsequently reviewed these logs, it found no threatening anomalies.	RFC_URE2 implemented manual monthly security log reviews.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100812	CIP-007-1	R6.5	RFC_URE3 self-reported an issue with CIP-007-1 R6.5 to Reliability*First.* RFC_URE3 maintained logs of system events related to cybersecurity but had no documentation to verify that they reviewed the security logs from its transmission management system.	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. RFC_URE3 protects its transmission management system with layers of defenses beginning with physical security access controls that isolate the hosts from unauthorized access and any potential vulnerabilities. In addition, RFC_URE3's parent company corporate networks were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions at all relevant times. These protections constitute a defense-in-depth strategy of protection that an intruder would have to overcome to gain access to RFC_URE3's transmission management system. In addition, although RFC_URE3 failed to review the security logs, the security logs for the transmission management system did exist. When RFC_URE3 subsequently reviewed these logs, it found no threatening anomalies.	RFC_URE3 implemented manual monthly security log reviews.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100783	CIP-004-1	R4.1	RFC_URE1 self-reported an issue with CIP-004-1 R4.1 to Reliability*First.* RFC_URE1 discovered that it failed to review all access lists of personnel who have authorized cyber or authorized unescorted physical access rights to Critical Cyber Assets (CCA). Specifically, RFC_URE1 failed to review the access list for a device at one substation.	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 factor. There were no individuals who should have been removed from the access list. All the personnel appropriately had authorized cyber or authorized unescorted physical access rights to CCAs.	RFC_URE1 began reviewing the CCA access lists for the device at issue and continued monitoring access rights to the device until the device was decommissioned. In addition, RFC_URE1 added the CCA access lists to the RFC_URE1 quarterly review of access rights until the device was decommissioned.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100784	CIP-005-1	R3.1	RFC_URE1 self-reported an issue with CIP-005-1 R4.1 to Reliability*First.* RFC_URE1 discovered that it failed to document and implement a monitoring process at each access point to a dial-up device. RFC_URE1's device was a dial-up accessible Critical Cyber Assets (CCA) that used a non-routable protocol. RFC_URE1's substations contained a device within an Electronic Security Perimeter, and due to oversight, RFC_URE1 failed to document and implement a process for monitoring access at this dial-up device.	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 individuals who had access to the device were properly authorized, had been trained, and had current personnel risk assessments. In addition, in order to access a device, an individual must have had a user identification and password that matched the user identification and password created solely for the device access. Further, although RFC_URE1 failed to monitor logs generated for this access point, it did generate the required logs for this access point to the dial-up device as of the compliance date.	RFC_URE1 documented the monitoring process for the security review and logging procedures for the device at issue. In addition, the device at issue was decommissioned.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100789	CIP-007-1	R1.1	RFC_URE1 self-reported an issue with CIP-007-1 R1.1 to Reliability*First.* RFC_URE1's relay access devices are identified as Critical Cyber Assets (CCA) and reside within the Electronic Security Perimeter (ESP). RFC_URE1 discovered that it had an issue with CIP-007-3 R1.1 for failing to have documentation or records to verify the initial testing that would ensure no adverse effects to existing security controls of the security configuration of the relay access devices.	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). However, the risk to the reliability of the BPS was mitigated by the following factors. Although RFC_URE1 failed to document the tests, RFC_URE1 did perform the tests to ensure that the new Cyber Assets did not adversely affect existing cybersecurity controls. Specifically, it utilized the same process for the devices during the installation process as they do for all CCAs, which includes reviewing the controls and testing the configuration of the Cyber Asset. In addition, RFC_URE1 performed a field test consisting of a remote verification of the correct functional configuration of the devices during the time of installation to confirm its standard configuration. Furthermore, the ports and services enabled on the relay access devices beyond those required were located within the ESP, further limiting access.	RFC_URE1 performed a scan of the relay access devices during its annual cyber vulnerability assessment. During that scan, RFC_URE1 compared required ports and services for the relay access devices with actual ports and services and performed testing to determine the necessary configuration changes. RFC_URE1's change control tool now documents the final disposition of enabled and disabled ports and services. RFC_URE1 performed the required changes to the relay access devices.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201100799	CIP-007-1	R1.1	RFC_URE2 self-reported an issue with CIP-007- R1.1 to Reliability*First.* RFC_URE2's relay access devices are identified as Critical Cyber Assets (CCA) and reside within the Electronic Security Perimeter (ESP). RFC_URE2 discovered that it had an issue with CIP-007-3 R1.1 for failing to have documentation or records to verify the initial testing that would ensure no adverse effects to existing security controls of the security configuration of the relay access devices.	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). However, the risk to the reliability of the BPS was mitigated by the following factors. Although RFC_URE2 failed to document the tests, RFC_URE2 did perform the tests to ensure that the new Cyber Assets did not adversely affect existing cybersecurity controls. Specifically, it utilized the same process for the devices during the installation process as they do for all CCAs, which includes reviewing the controls and testing the configuration of the Cyber Asset. In addition, RFC_URE2 performed a field test consisting of a remote verification of the correct functional configuration of the devices during the time of installation to confirm its standard configuration. Furthermore, the ports and services enabled on the relay access devices beyond those required were located within the ESP, further limiting access.	RFC_URE2 performed a scan of the relay access devices during its annual cyber vulnerability assessment. During that scan, RFC_URE2 compared required ports and services for the relay access devices with actual ports and services and performed testing to determine the necessary configuration changes. RFC_URE2's change control tool now documents the final disposition of enabled and disabled ports and services. RFC_URE2 performed the required changes to the relay access devices.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) Southeastern Power Administration (SEPA)	NCRXXXXX	SERC201000533	CIP-002-1	R1	The SERC CIP Spot-Check team reported that SERC_URE1 had an issue with CIP-002-1 R1, stating that historical versions of SERC_URE1's risk-based assessment methodology (RBAM) did not consider the assets listed in R1.2.1 through R1.2.7. SERC staff reviewed SERC_URE1 historical versions of its RBAM and Critical Asset lists and determined that SERC_URE1 did not consider the assets listed in R1.2.1 through R1.2.7 in its RBAM.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in CIP-002-4; and 2. SERC_URE1 is a partial requirements supplier. SERC_URE1 does not own any transmission or generation assets.	SERC staff verified that SERC_URE1 completed the following actions: SERC_URE1 revised its RBAM to specifically address the criteria listed in CIP-002-1 R1.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC201000742	CIP-005-2	R3	SERC_URE2 self-reported an issue with CIP-005-2 R3.2, stating that it had failed to review access logs for attempts at or actual unauthorized access within ninety calendar days as required. SERC staff learned that SERC_URE2 completed a review of its access logs, but due to an error in data entry, the date of completion entered in its internal tracking mechanism was incorrect. Due to the error in data entry, SERC_URE2 actually completed its third quarter review one day late, 91 calendar days after the previous review.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE2 conducted its review one day late and found no attempts at or actual unauthorized access in the access logs; and 2. SERC_URE2 had a process in place for reviewing access logs but was late in completing that review due to an error in entering the date of the previous access log review.	SERC staff verified that SERC_URE2 completed the following actions: 1. SERC_URE2 shortened the interval between access log reviews to 75 days to provide a 15 day buffer on the 90-day requirement. 2. SERC_URE2 revised and implemented enhancements to its manual access log review procedure, which add more detail to the following key steps in the process: (a) gathering access log data for review; (b) analyzing the access log data; (c) recording the results of the access log review; (d) calculating and tracking the next access log review milestone dates; and (e) independently reviewing access log evidence and calculated dates for the next review period. 3. The enhancements to the access log review procedure also ensure that the data obtained for access log reviews always overlap with the previous review period and all pertinent dates used to ensure compliance are individually tracked.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC201000741	CIP-005-2	R3	SERC_URE3 self-reported an issue with CIP-005-2 R3.2, stating that it had failed to review access logs for attempts at or actual unauthorized access within ninety calendar days as required. SERC staff learned that SERC_URE3 completed a review of its access logs, but due to an error in data entry, the date of completion entered into its internal tracking mechanism was incorrect. Due to the error in data entry, SERC_URE3 actually completed its third quarter review one day late, 91 calendar days after the previous review.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE3 conducted its review one day late and found no attempts at or actual unauthorized access in the access logs; and 2. SERC_URE3 had a process in place for reviewing access logs but was late in completing that review due to an error in entering the date of the previous access log review.	SERC staff verified that SERC_URE3 completed the following actions: 1. SERC_URE3 shortened the interval between access log reviews to 75 days to provide a 15 day buffer on the 90-day requirement; 2. SERC_URE3 revised and implemented enhancements to its manual access log review procedure, which add more detail to the following key steps in the process: (a) gathering access log data for review; (b) analyzing the access log data; (c) recording the results of the access log review; (d) calculating and tracking the next access log review milestone dates; and (e) independently reviewing access log evidence and calculated dates for the next review period. 3. The enhancements to the access log review procedure also ensure that the data obtained for access log reviews always overlap with the previous review period and all pertinent dates used to ensure compliance are individually tracked.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPPRE_URE1) City Of Gardner (Gardner)	NCRXXXXX	SPP201100626	CIP-002-3	R1.1	During a CIP audit of SPPRE_URE1, the SPP RE CIP audit team discovered a possible issue with CIP-002-3 R1.1. The audit team found that while SPPRE_URE1 developed and maintained a risk-based methodology (RBAM) to identify Critical Assets (CAs), which included a defined procedure for performing its RBAM and included the considerations listed in CIP-002-3 R1.2, SPPRE_URE1 failed to fully describe its evaluation criteria for identifying CAs, thereby presenting an issue with CIP-002-3 R1.1.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although SPPRE_URE1 did not fully describe its evaluation criteria for identifying CAs in its RBAM, SPPRE_URE1 did have an RBAM that it documented and maintained. Furthermore, SPPRE_URE1 was able to apply its RBAM sufficiently to determine that it did not own any CAs or any Critical Cyber Assets (CCAs). The subsequent changes implemented by SPPRE_URE1 to fully describe its evaluation criteria in its RBAM did not result in the identification of any additional CAs. Therefore, SPP RE determined that SPPRE_URE1's procedure did not fully describe the evaluating criteria for identifying CAs, in accordance with the applicable Requirement.	SPPRE_URE1 implemented an addition to its RBAM that includes specific criteria for evaluating and identifying CAs. The specific criteria addresses the requirements of CIP-002-3 R1.1.

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)	NCRXXXXX	TRE201100473	CIP-004-3	R2	Texas RE_URE1 self-reported a possible compliance issue with CIP-004-3 R2. Texas RE_URE1 stated that it hired a planning supervisor at one of its plants. Four days later, the supervisor was granted authorized unescorted physical access to Texas RE_URE1's Physical Security Perimeters (PSPs) containing Critical Cyber Assets (CCAs), although the supervisor had not completed Texas RE_URE1's cyber security training program yet. Texas RE also determined that this compliance issue was the result of a combination of (1) the two employees that were authorizing access and issuing the access badges were relatively new in their roles; and (2) the access request and authorization form did not require a confirmation of the date when cyber security training was completed. The supervisor's access was revoked approximately six months later, the same day Texas RE_URE1 discovered the compliance issue. Therefore, Texas RE determined that the issue was from when access was granted to the supervisor to when access was revoked. The supervisor completed the required training and access was given back to him a week after the access was revoked.	This compliance issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because the risk was mitigated by several factors. First, the supervisor had undergone partial training prior to receiving authorized unescorted physical access to Texas RE_URE1's PSPs containing CCAs. Texas RE_URE1's code of conduct and other corporate policies were provided to the supervisor in question prior to granting him such access. These corporate policies contain information that mirror many of the items included in Texas RE_URE1's Critical Infrastructure Protection (CIP) training, thereby reducing the risk to the BPS presented by the supervisor's lack of required cyber security training. Second, the supervisor's personnel risk assessment (PRA) was successfully completed the prior year, prior to granting him access to the PSPs. Third, the supervisor had physical access, but no cyber access to the CCAs for the period in question, and his job did not require any physical or cyber interaction with the CCAs. Also, Texas RE determined that there was only a limited possibility of granting access to Texas RE_URE1's PSPs containing CCAs prior to completing the required training because of the relatively small number of new applications for such access. Texas RE determined that the potential number of such improper access authorizations was reduced by the fact that the employees involved in authorizing access and issuing badges knew that cyber security training was required prior to granting authorization. Therefore, only one isolated incident of noncompliance with this Standard has occurred during the issue period.	Texas RE_URE1 revoked the supervisor's access the same day the violation was discovered and granted access again when the supervisor completed the required training. Additional training was completed for those individuals responsible for managing and granting access to NERC CIP protected areas at the plant in question. Texas RE_URE1's NERC CIP access authorization form was modified to include a verification of the date that cyber security training was complete and required that training was confirmed before access was granted. Additional cyber security training was conducted for other plant employees in order to increase awareness of NERC CIP cyber security requirements. Finally, Texas RE_URE1 completed a company-wide review of its NERC CIP access management and control procedures to avoid future instances of noncompliance with this Standard. Texas RE verified completion of these mitigation activities.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1) Idaho Wind Partners 1, LLC (IWPL)	NCRXXXXX	WECC2012009958	CIP-003-3	R2	During an internal review of its Compliance Program, WECC_URE1 self-reported a possible issue of CIP-003-3 R2. According to the Self-Report, WECC_URE1 failed to assign a single manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standard CIP-002-3 through CIP-009-3 for approximately three months. Although WECC_URE1 did not assign a CIP senior manager, it has self-certified that it did not own any Critical Assets (CAs) or Critical Cyber Assets (CCAs). In the past, WECC_URE1 was not required to be compliant with CIP-003 through CIP-009 because it did not have CAs or CCAs. This was accurate until April 1, 2010, when CIP-003-2 became enforceable for WECC_URE1 due to changes in Section 4.2.3 of CIP-003-2. The change required in Version two was also required when Version three became enforceable on October 1, 2010. The change requires CIP-003-3 R2 to apply to all Responsible Entities, including Responsible Entities that have no CCAs. WECC_URE1 failed to notice this change in the Standard and as a result failed to assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3, as required by CIP-003-3 R2.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Although WECC_URE1 failed to assign a senior manager as required by CIP-003-3 R2, WECC determined that the issues posed a minimal risk to the reliability of the bulk power system because WECC_URE1 has a null list of CAs or CCAs. Additionally, WECC_URE1 does not operate any facilities that would meet any of the Critical Asset identification criteria.	WECC verified that WECC_URE1 had completed the following mitigating activities: WECC_URE1 assigned a senior manager with the overall responsibility and authority for leading and managing the implementation of and adherence to CIP-002 through CIP-009. WECC_URE1's general compliance manager was trained on CIP standards and his responsibilities to ensure that the Cyber Security Assignment is properly documented and stored.

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 2 (WECC_URE2)	NCRXXXXX	WECC2012009103	CIP-005-1	R1	WECC_URE2 submitted a Self-Report addressing possible noncompliance with CIP-005 R1. WECC_URE2 failed to ensure it provided all the protections specified in CIP-005 R1.5 to two token servers used in the access control and monitoring of Electronic Security Perimeters (ESPs). Specifically, WECC_URE2 did not have a list of individuals with access to the token servers, thus, WECC_URE2 was not able to provide evidence of compliance for four sub-requirements of CIP-007 R5 (i.e., CIP-007 R5.1.1, CIP-007 R5.1.3, CIP-007 R5.2.2, CIP-007 R5.2.3). WECC_URE2 did provide CIP-007 R5.3 protections and additionally submitted an acceptable and applicable Technical Feasibility Exception for CIP-007 R5.3.2. WECC_URE2 did not conduct cyber vulnerability assessments on these devices (pursuant to CIP-007 R8), did not conduct an annual review pursuant to CIP-007 R9 and did not have or exercise a recovery plan nor test the devices backup media at least annually pursuant to CIP-009 R1, R2, and R5. Accordingly, WECC determined WECC_URE2 had a possible issue of CIP-005-1 R1.5. Although Enforcement determined WECC_URE2 did not apply the above-listed protections to two servers, the devices associated with the noncompliance support WECC_URE2's multi-factor authentication security protocols and are limited to a single factor of the authentication protocol. Further, these devices are part of WECC_URE2's defense-in-depth security architecture. Thus, if these token servers were compromised, a valid username and password would still be required to gain access into WECC_URE2. Therefore, the Cyber Assets inside the ESPs would remain protected.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. Despite not treated in accordance with the protective measures specified in CIP-005-1 R1.5, the devices in scope had malware prevention tools, restricted logical access with active directory, used tripwire file monitoring, and were located in a Physical Security Perimeter (PSP). Further, although WECC_URE2 did not have a recovery plan for the devices, it did maintain backups that could have been used to recover the token servers. The devices were located in a secure network and behind restrictive firewalls. Additionally, the devices were configured to send all syslogs to the entity's system event monitoring servers; these servers are configured for automated alerting. Most importantly, the devices in scope were responsible for only one of the two factors required to gain access to the ESPs. To gain access into the ESPs, a user requires a valid user name and password from active directory, and a "token" from the devices in scope. Thus, if these token servers were compromised, a valid username and password would still be required to gain access into the ESPs. Therefore, the Cyber Assets inside the ESPs would remain protected, as access into the ESPs requires both factors. Additionally, all individuals with access to CCAs had current training and PRAs.	WECC_URE2 evaluated the assets to ensure WECC_URE2 afforded protective measures specified in CIP-003, CIP-004 R3, CIP-005 R2, R3, CIP-006 R3 to the devices. WECC_URE2 added the Cyber Assets to its list of Cyber Assets used for electronic access control and monitoring. WECC_URE2 completed its evaluation of the devices and the applicable protective measures. WECC_URE2 ensured it afforded these devices the protective measures specified in CIP-008 R1, R2, CIP-009 R1, R2, R3, R4, R5, and CIP-007 R1, R3, R4, R5, R6, R7, R8, R9.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012009104	CIP-005-1	R2	WECC_URE2 submitted a Self-Report addressing possible noncompliance with CIP-005 R2. WECC_URE2 did not ensure all its access control devices displayed an appropriate use banner, thus WECC determined WECC_URE2 was in noncompliance with CIP-005-1 R2.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. All Critical Cyber Assets (CCAs) inside the ESP displayed an appropriate use banner upon interactive access and were located in a Physical Security Perimeter and an Electronic Security Perimeter, and thus afforded the protections of CIP-005 and CIP-006. Further, if inappropriate use was suspected, WECC_URE2's tripwire file monitoring is configured to detect any changed files on the CCAs. The devices were also configured to send all system logs to the entity's system event monitoring server which is configured for automated alerting upon unauthorized access attempts. Additionally, all individuals with access to CCAs had current training and PRAs.	WECC_URE2 evaluated the assets to ensure WECC_URE2 afforded protective measures specified in CIP-003, CIP-004 R3, CIP-005 R2, R3, CIP-006 R3 to the devices. WECC_URE2 added the Cyber Assets to its list of Cyber Assets used for electronic access control and monitoring. WECC_URE2 completed its evaluation of the devices and the applicable protective measures. WECC_URE2 ensured it afforded these devices the protective measures specified in CIP-008 R1, R2, CIP-009 R1, R2, R3, R4, R5, and CIP-007 R1, R3, R4, R5, R6, R7, R8, R9.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3) NorthWestern Corporation (NWC)	NCRXXXXX	WECC2012009975	CIP-005-1	R2	WECC conducted an onsite Compliance Audit (Audit) of WECC_URE3. During a site tour conducted by WECC of WECC_URE3's facilities, WECC identified three electronic access control devices that did not display an appropriate use banner on the screen upon all interactive access attempts. The three devices identified during the Audit were electronic access control devices required to display an appropriate use banner pursuant to R2.6. WECC_URE3's failure to implement a use banner that displays upon all interactive access attempts constitutes an issue of CIP-005-1 R2.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. The risks posed by WECC_URE3 noncompliance are limited given compensating measures in place during the noncompliance period. WECC_URE3 has an in-depth defense structure to ensure electronic security. This includes network segmentation within ESPs. All Cyber Assets and Critical Cyber Assets are secured behind firewalls wherein access is controlled, logged and monitored. All personnel with access to each of the three devices have completed Cyber Security training and have completed personnel risk assessments. Each of the three devices is password protected.	WECC_URE3 installed an appropriate use banner on the three devices. The appropriate use banner is displayed on devices upon all interactive access attempts.
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC2011008655	CIP-006-1	R1	WECC_URE4 submitted a Self-Report citing noncompliance with CIP-006-1 R1. Specifically, WECC_URE4 reported that it failed to ensure seven Cyber Assets within an Electronic Security Perimeter (ESP) were also located in a Physical Security Perimeter (PSP) per CIP-006-1 R1. WECC determined that the seven devices in scope of the Self-Report were not Critical Cyber Assets. Further, WECC determined that none of the devices were ESP access points. WECC determined that the seven devices were switches and firewalls used to direct, restrict and monitor traffic inside the ESP. Accordingly, WECC determined that WECC_URE4 failed to secure seven non-critical Cyber Assets within PSPs.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. The devices in scope were not Critical Cyber Assets or ESP access points and had limited connectivity within the ESP. Further, the seven devices were physically secured within locked closets that afforded a number of protections. The closets were secured by magnetic/electronic locks that opened using an authorized access badge. The closets resided in a secured facility that was monitored on a 24/7 basis. Access points to the facility were electronically monitored and alarmed.	WECC_URE4 remediated the issue by securing the seven Cyber Assets within an identified PSP.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electric Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2012009452	CIP-005-3	R2	WECC_URE5 submitted a Self Certification citing possible noncompliance with CIP-005-3 R2. Specifically, WECC_URE5 reported that it commissioned three devices provisioning Electronic Security Perimeter (ESP) access control and monitoring without having filed a Technical Feasibility Exception (TFE) for CIP-005-3 R2.6. CIP-005-3 R2.6 requires entities to ensure that devices provisioning access control and monitoring to the ESP, where technically feasible, display an appropriate use banner upon all interactive attempts. In this case, WECC determined that WECC_URE5 failed to file a timely TFE for three devices on which it was not technically feasible to display an appropriate use banner as required by CIP-005-3 R2.6.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. The three devices were secured behind firewalls that did display the banner. The devices were secured within an ESP and a Physical Security Perimeter. Electronic and physical access thereto was, therefore, controlled and monitored. A limited number of personnel were granted electronic or physical access rights to the devices. These individuals all completed personnel risk assessments and cybersecurity training.	WECC_URE5 filed a TFE for each of the three devices identified herein. WECC reviewed WECC_URE5's TFE and issued a notice of TFE acceptance.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 6 (WECC_URE6)	NCRXXXXX	WECC2011008670	CIP-007-1	R4	CIP-007-1 R4 requires WECC_URE6 to use anti-virus software and other malicious software (malware) prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s). WECC_URE6 submitted a Self-Report for possible noncompliance with CIP-007-1 R4. WECC reviewed the Self-Report and determined that WECC_URE6 was in noncompliance with CIP-007-1 R4 for its failure to have anti-virus and other malware software installed. Related to this Self-Report, WECC_URE6 submitted Technical Feasibility Exception Requests (TFEs), addressing its technical infeasibility to install anti-virus and other malware software, to comply with CIP-007-1 R4. WECC approved the TFE requests. Based on the technically feasible language, WECC determined that WECC_URE6's approved TFE requests satisfied the requirements of CIP-007-1 R4. However, as a result of the late filing date, WECC determined WECC_URE6 was in noncompliance with CIP-007-1 R4.	WECC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system. All devices are located within an ESP and a Physical Security Perimeter (PSP) with no direct connection to the internet or the use of email. Also, anti-virus software is installed on all other devices in the ESP and there is 24/7 monitoring and logging of physical and cyber access to these devices. Additionally, the ESPs have intrusion protection system sensors to inspect network traffic at the access points.	WECC_URE6 filed the TFE, WECC approved the Part A and Part B TFE.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 7 (WECC_URE7)	NCRXXXXX	WECC201102981	CIP-007-1	R4	WECC_URE7 self-certified a potential remediated issue of CIP-007-1 R4. WECC contacted WECC_URE7 to discuss its self-certification. WECC_URE7 stated that it failed to install anti-virus software and other malware prevention tools on twelve of its Critical Cyber Assets (CCAs). The CCAs are human-machine interfaces (HMI) that control gas compressors, analyzers, and facilitate programmable logic controllers that manage blackstart generators. The HMIs involved utilized operating systems that did not support anti-virus and malware prevention tools. As a result, it was technically infeasible for WECC_URE7 to install anti-virus and malware prevention tools on the devices involved.	WECC_URE7 provided WECC evidence from its vendor that substantiated the inability to install anti-virus and malware prevention tools on these devices. WECC determined this remediated issue posed a minimal risk to the reliability of the bulk power system. The devices were located inside of an Electronic Security Perimeter and the individuals who had access to the devices had personnel risk assessments (PRAs) and CIP training.	WECC_URE7 removed the routable connectivity of these devices and serially connected them to its Electronic Security Perimeter.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 8 (WECC_URE8)	NCRXXXXX	WECC2011008635	CIP-005-1	R2	WECC audited the WECC_URE8's compliance with CIP-005-1 R2. At the Audit, WECC_URE8 produced an Electronic Security Perimeter (ESP) architectural diagram detailing the configurations of its ESP at its substations. The diagrams the entity produced exemplified separate ESPs at each substation. Based on a review of these diagrams and an evaluation of WECC_URE8's individual ESPs at each of its substations, the Audit Team concluded that WECC_URE8 failed to implement default restrictions to its substation ESP access points as required by CIP-005-1 R2. In addition, the Audit Team concluded that WECC_URE8 failed to restrict traffic to specified ports and services on the substations ESP access points to all Cyber Assets with the ESP. Although WECC_URE8's architectural diagrams reflect individual substation ESPs and, as individual substation ESPs WECC_URE8 failed to implement appropriate access point controls, but it has in place a larger ESP that encompasses all the substations involved and does have appropriate access point controls. WECC_URE8 has implemented a security configuration on the larger ESP that ensures that all traffic to and from the substations involved are protected by a firewall with restrictive access controls.	Although WECC_URE8 failed to implement proper control as access points to an ESP which could allow unauthorized access to Critical Cyber Assets, WECC determined that the issue posed a minimal risk to the reliability of the bulk power system. In this instance, WECC_URE8 utilized a firewall at each substation. All traffic is decrypted and forced into a sub-interface on the firewall for rules processing. The firewall contains restrictive controls for each interface, thus ensuring only specific access is allowed based upon IP addresses and specific ports/services. In addition, WECC_URE8 has access control lists that deny access by default.	WECC_URE8 utilizes the firewall at each substation. All traffic is decrypted and forced into a sub-interface on the firewall for rules processing. The firewall contains restrictive controls for each interface, thus ensuring only specific access is allowed based upon IP addresses and specific ports/services. In addition, WECC_URE8 has implemented access control lists that deny access by default.

Document Accession #: 20120629-5272 Filed Date: 06/29/2012

Document Content(s)