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

Re: FOIA No. FY19-30
Thirty Seventh Determination Letter
Release

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated 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. RC12-8, 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 RC12-8.

With respect to the remaining identities of UREs contained in RC12-8, 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 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 RC12-8 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 13:15:41 -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

Document Accession #: 20120229-5270 Filed Date: 02/29/2012

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC12-8

Calpine Energy Services (CALP)-see .pdf page 25

Calpine Corporation (CALPGO)-see .pdf page 25

CPS Energy-see .pdf page 25

City of Fredericksburg-see .pdf page 27

February 29, 2012

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 24 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

This FFT resolves 46 possible violations[5] of 18 Reliability Standards that posed a lesser risk (minimal to moderate) 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 statement of completion of the mitigation activities has been submitted by the respective Registered Entities.

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

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

As discussed below, this FFT includes 46 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined enforcement processes for occurrences that posed lesser risk to the BPS.[6] Resolution of these lesser 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 statement 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 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.

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 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.

[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).

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 30326-1001 (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 30326-1001
(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 FEBRUARY 2012 FIND FIX AND TRACK REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

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

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

FOR 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 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 SPP RE:

Stacy Dochoda*
General Manager
Southwest Power Pool Regional Entity
16101 St. Vincent Way, Ste 103
Little Rock, AR 72223
(501) 688-1730
(501) 821-8726 – facsimile
sdochoda.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
February 29, 2012

Take notice that on February 29, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding twenty-four (24) Registered Entities in six (6) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE 1)	NCRXXXXX	FRCC2011007584	BAL-005-0.1b	R10	The entity self-reported an issue with BAL-005-0.1b R10. In the first instance, a transaction was tagged as a Dynamic Schedule and from midnight until 10:00 the Dynamic Schedule was not included in the entity's Net Scheduled Interchange for the Area Control Error (ACE) equation, as required by the Standard. In the second instance, another transaction was tagged as a Dynamic Schedule. The transaction ran as a Dynamic Schedule from 14:00 on the first day until midnight on the sixth day. From 00:00 on the first day until 23:59 on the sixth day, the Dynamic Schedule was not included in the entity's Net Scheduled Interchange for the ACE equation.	FRCC determined that this issue did not pose serious or substantial risk and posed minimal risk to the reliability of the bulk power system (BPS) because the magnitude of the Dynamic Schedules was less than 30 MW. There were no calls for reserves by the FRCC Reliability Coordinator for reliability reasons during the period of these events. In addition, those Dynamic Schedules were requested due to commercial drivers rather than reliability-related needs. Although the entity has violated this Standard previously, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The prior violation occurred two years prior to the instant remediated issue. Further, the prior violation involved a specific problem caused by confusion regarding the agreed-upon ramp duration in the region, and as such is unrelated to the instant conduct. Following the prior violation, the entity notified marketers to refrain from submitting tags with a blank ramp duration, trained energy system operators to deny any tag with an incorrect or blank ramp rate, implemented daily after-the-fact monitoring to ensure ramp durations of tags are not blank and match schedules, implemented an automatic tag validation tool to flag as failed all tags with a blank ramp duration, and investigated potential automatic transfer of information from tags to the energy tracking system.	The entity completed mitigation activities including: 1) Investigated options to alert the operator whether a tag is a Dynamic Schedule or a normal schedule and implemented a computer program to flag the Dynamic Schedules and a procedure for the operators to become aware of the computer alerts system; 2) Documented the procedure to cover any new Dynamic Schedule implementation that includes training and testing prior to implementation; 3) Reviewed the procedure with support personnel regarding proper implementation of Dynamic Schedules; and 4) Trained the operators on the new alert for Dynamic Schedules. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE 2)	NCRXXXXX	FRCC2011007253	CIP-005-2	R5; R5.2	During a spot check, FRCC determined that the entity had an issue with CIP-005-2 R5. The entity's evidence was not sufficient to demonstrate that the entity updated the documentation to reflect the modification of the network or controls within 90 calendar days of the change. The entity's restoration plan included back-up requirements for intrusion protection devices which were removed the year before the spot check. The documentation was updated less than two years after the devices were removed.	FRCC determined that this issue did not pose serious or substantial risk and posed minimal risk to the reliability of the bulk power system (BPS) because the lack of updated documentation was mitigated by the fact that all entity personnel were adequately trained in recovery of the newly installed intrusion protection devices which were appropriately configured.	The entity completed mitigation activities including modifying the Critical Cyber Asset change management process and including steps for updating documents within the required period.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE 2)	NCRXXXXX	FRCC2011007258	CIP-007-1	R4; R4.2	During a spot check, FRCC determined that the entity had an issue with CIP-007-1 R4. The entity's evidence was sufficient to demonstrate that the entity submitted Technical Feasibility Exceptions (TFEs) for some of its devices. The FRCC spot check team reviewed entity documents and concluded that additional devices needed TFEs. Thus, the entity failed to submit TFEs for 15% of devices requiring TFEs. For these additional devices, the entity could not demonstrate that it documented a process for the update of anti-virus and malware prevention signatures which would address testing and installing the signatures.	FRCC determined that this issue did not pose serious or substantial risk and posed minimal risk to the reliability of the bulk power system (BPS) because the entity submitted TFEs for 85% of devices requiring TFEs. The incorrect accounting of the devices was an oversight and comparable security measures were enabled for the complete set of devices. Further, the entity had implemented a process for the update of anti-virus and malware prevention signatures which addressed testing and installing the signatures and the issue relates only to the failure to document the process.	The entity completed mitigation activities and submitted a new TFE for the remaining devices. The entity also updated the compliance documentation to include a process for the update of anti-virus and malware prevention signatures which addresses testing and installing the signatures.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009040	CIP-007-2a	R9	During a NPCC CIP compliance audit, it was found that the entity had an issue with CIP-007-2a R9. NPCC determined that two of the entity's information security standard documents were not corrected to change its 90-day requirement to a 30-day requirement as required by the change in CIP-007-2a R9. The entity's information security standard documents were not corrected to change its 90-day requirement to a 30-day requirement, as required by the change in CIP-007-2a R9; however, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes in CIP-007-3. The entity's NERC CIP information security standard documents are single corporate documents that are relied upon by multiple affiliated registered entities for compliance with CIP-007-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because there were no system or control changes that occurred during the 8-month period in which the plan used the incorrect 90-day requirement. In addition, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including updating the entity's parent company's information security standard documents by changing the ninety calendar day update requirement to the thirty calendar day update requirement. NPCC verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008449	CIP-007-2a	R9	The entity self-reported to NPCC an issue with CIP-007-2a R9. During a CIP compliance audit of the entity's subsidiary, NPCC determined that the entity failed to correct two of its information security standard documents to change its 90-day requirement to a 30-day requirement, as required by the change in CIP-007-2a R9. The entity's information security standard documents were not corrected to change its 90-day requirement to a 30-day requirement as required by the change in CIP-007-2a R9; however, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes in CIP-007-3. The entity's NERC CIP information security standard documents are single corporate documents that are relied upon by multiple affiliated registered entities for compliance with CIP-007-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because there were no system or control changes that occurred during the 8-month period in which the plan used the incorrect 90-day requirement. In addition, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including updating the entity's parent company's information security standard documents by changing the ninety calendar day update requirement to the thirty calendar day update requirement. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008337	CIP-007-2a	R9	The entity self-reported to NPCC an issue with CIP-007-2a R9. During a CIP compliance audit of the entity's affiliate, NPCC determined that the entity failed to correct two of its information security standard documents to change its 90-day requirement to a 30-day requirement, as required by the change in CIP-007-2a R9. The entity's information security standard documents were not corrected to change its 90-day requirement to a 30-day requirement as required by the change in CIP-007-2a R9; however, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes in CIP-007-3. The entity's NERC CIP information security standard documents are single corporate documents that are relied upon by multiple affiliated registered entities for compliance with CIP-007-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because there were no system or control changes that occurred during the 8-month period in which the plan used the incorrect 90-day requirement. In addition, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including updating the entity's parent company's information security standard documents by changing the ninety calendar day update requirement to the thirty calendar day update requirement. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011008451	CIP-007-2a	R9	The entity self-reported to NPCC an issue with CIP-007-2a R9. During a CIP compliance audit of the entity's affiliate, NPCC determined that the entity failed to correct two of its information security standard documents to change its 90-day requirement to a 30-day requirement, as required by the change in CIP-007-2a R9. The entity's information security standard documents were not corrected to change its 90-day requirement to a 30-day requirement as required by the change in CIP-007-2a R9; however, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes in CIP-007-3. The entity's NERC CIP information security standard documents are single corporate documents that are relied upon by multiple affiliated registered entities for compliance with CIP-007-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because there were no system or control changes that occurred during the 8-month period in which the plan used the incorrect 90-day requirement. In addition, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including updating the entity's parent company's information security standard documents by changing the ninety calendar day update requirement to the thirty calendar day update requirement. NPCC verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008444	CIP-003-1	R1; R1.3	The entity self-reported to NPCC an issue with CIP-003-1 R1. During a NPCC CIP audit of the entity's subsidiary, it was found that the entity's cyber security policy was not signed by the senior manager assigned pursuant to CIP-003-2 R2, as required by the Standard. The cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-003-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the cyber security policy was not signed by the senior manager assigned pursuant to CIP-003 R2, it was reviewed by another department, who performs an annual review covering all NERC CIP-related information security requirements, and signed by another officer. This other officer was designated by the senior manager as his/her delegate pursuant to CIP-003 R2.3. Although the entity's subsidiary has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including reviewing and receiving approval of the cyber security policy by the senior manager assigned pursuant to CIP-003 R2. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011008445	CIP-003-1	R1; R1.3	The entity self-reported to NPCC an issue with CIP-003-1 R1. During a NPCC CIP audit of the entity's affiliate, it was found that the entity's cyber security policy was not signed by the senior manager assigned pursuant to CIP-003-2 R2, as required by the Standard. The cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-003-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the cyber security policy was not signed by the senior manager assigned pursuant to CIP-003 R2, it was reviewed by another department, who performs an annual review covering all NERC CIP-related information security requirements, and signed by another officer. This other officer was designated by the senior manager as his/her delegate pursuant to CIP-003 R2.3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including reviewing and receiving approval of the cyber security policy by the senior manager assigned pursuant to CIP-003 R2. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011008443	CIP-003-1	R1; R1.3	The entity self-reported to NPCC an issue with CIP-003-1 R1. During a NPCC CIP audit of the entity's affiliate, it was found that the entity's cyber security policy was not signed by the senior manager assigned pursuant to CIP-003-2 R2, as required by the Standard. The cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-003-2, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the cyber security policy was not signed by the senior manager assigned pursuant to CIP-003 R2, it was reviewed by another department, who performs an annual review covering all NERC CIP-related information security requirements, and signed by another officer. This other officer was designated by the senior manager as his/her delegate pursuant to CIP-003 R2.3. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including reviewing and receiving approval of the cyber security policy by the senior manager assigned pursuant to CIP-003 R2. NPCC verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008452	CIP-008-2	R1; R1.4	The entity self-reported to NPCC an issue with CIP-008-2 R1. During a NPCC CIP compliance audit of the entity's subsidiary it was found that the subsidiary's information security standard incident management document was approved to require a process for updating the Cyber Security Incident response plan within thirty days of any changes, as required by the Standard. This was done seventy days after its obligation to meet the 30-day requirement. The entity's cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-008-2 R1.4, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the information security standard incident management document was updated within a short period of time - less than three months after the ninety calendar day update requirement changed to the thirty calendar day update requirement. No interim and future risks were identified. Although the entity's subsidiary has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including the entity's information security standard incident management document was approved with the update to require a process for updating the Cyber Security Incident response plan within thirty days of any changes. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 4 (NPCC_URE4)	NCRXXXXX	NPCC2011008453	CIP-008-2	R1; R1.4	The entity self-reported to NPCC an issue with CIP-008-2 R1. During a NPCC CIP compliance audit of the entity's affiliate, it was found that the affiliate's information security standard incident management document was approved to require a process for updating the Cyber Security Incident response plan within thirty days of any changes, as required by the Standard. This was done seventy days after its obligation to meet the 30-day requirement. The entity's cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-008-2 R1.4, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the information security standard incident management document was updated within a short period of time - less than three months after the ninety calendar day update requirement changed to the thirty calendar day update requirement. No interim and future risks were identified. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including the entity's parent company's information security standard incident management document was approved with the update to require a process for updating the Cyber Security Incident response plan within thirty days of any changes. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009041	CIP-008-2	R1; R1.4	During a NPCC CIP compliance audit, it was determined that the entity had an issue with CIP-008-2 R1. NPCC determined that the entity's information security standard incident management document was approved to require a process for updating the Cyber Security Incident response plan within thirty days of any changes, as required by the Standard. This was done seventy days after its obligation to meet the 30-day requirement. The entity's cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-008-2 R1.4, including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the information security standard incident management document was updated within a short period of time - less than three months after the ninety calendar day update requirement changed to the thirty calendar day update requirement. No interim and future risks were identified. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including the entity's parent company's information security standard incident management document was approved with the update to require a process for updating the Cyber Security Incident response plan within thirty days of any changes. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008454	CIP-009-1	R4	The entity self-reported to NPCC an issue with CIP-009-1 R4. During a NPCC CIP compliance audit of the entity's subsidiary it was found that there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storing information required to successfully restore Critical Cyber Assets (CCAs). The entity's cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-009-1 R4 including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because evidence was provided that although there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storage of information required to successfully restore CCAs, the backup and storage of information required to successfully restore CCAs was taking place. Although the entity's subsidiary has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including revising its disaster recovery procedures to include references to its change control and configuration procedure. The entity also revised this change control and configuration procedure to address CIP-009 R4 backup and restore requirements. NPCC verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009042	CIP-009-1	R4	During a NPCC CIP compliance audit, it was determined that the entity had an issue with CIP-009-1 R4. NPCC determined that there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storing information required to successfully restore Critical Cyber Assets (CCAs). The entity's cyber security policy is a single corporate document that is relied upon by multiple affiliated registered entities for compliance with CIP-009-1 R4 including the entity.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because evidence was provided that although there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storage of information required to successfully restore CCAs, the backup and storage of information required to successfully restore CCAs was taking place. Although the entity's affiliate has had an issue with this Standard previously, which was submitted in a prior FFT Report, the instant remediated issue nonetheless does not represent recurring conduct by the registered entity. The instant remediated issue and the prior remediated issue arose from the same conduct and was therefore not considered to be an aggravating factor.	The entity completed mitigation activities including revising its disaster recovery procedures to include references to its change control and configuration procedure. The entity also revised this change control and configuration procedure to address CIP-009 R4 backup and restore requirements. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2011008517	CIP-005-1	R4	During a joint compliance audit conducted by NPCC and another region, NPCC determined that the entity failed to complete a cyber vulnerability assessment in accordance with CIP-005-1 R4. NPCC determined that the entity completed its first formal cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter (ESP) eleven months past the required compliance date. The other region also found that the same conduct gave rise to an issue for an affiliate of the entity. NPCC did not consider the affiliate's issue an aggravating factor, as the issues arose from the same conduct.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the formal annual cyber vulnerability assessment by its required compliance date, it did complete most of the work required by CIP-005-1 R4.1 through R4.4, including continually reviewing and hardening its ESP firewalls.	The entity completed the cyber vulnerability assessment. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2011008518	CIP-007-1	R8	During a joint compliance audit conducted by NPCC and another region, NPCC determined that the entity failed to complete a cyber vulnerability assessment in accordance with CIP-007-1 R8. NPCC determined that the entity completed its first formal cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter (ESP) eleven months past the required compliance date. The other region also found that the same conduct gave rise to an issue for an affiliate of the entity. NPCC did not consider the affiliate's issue an aggravating factor, as the issues arose from the same conduct.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the formal annual cyber vulnerability assessment by its required compliance date, it did complete most of the work required by CIP-007-1 R8.1 through R8.4, including continually reviewing and hardening its ESP firewalls. The entity also provided examples of actions such as approved purchase orders and statements of work which showed that the elements of the vulnerability assessment were being exercised and documented before the compliant status due date.	The entity completed the cyber vulnerability assessment. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2011008519	CIP-006-1	R1; R1.8	During a joint compliance audit conducted by NPCC and another region, NPCC determined that the entity had an issue with CIP-006-1 R1. CIP-006-1 R1.8 requires Cyber Assets used in the access control and monitoring of the Physical Security Perimeter to be afforded the protections required by various CIP standards, including a vulnerability assessment as required by CIP-007-1 R8. NPCC determined that the entity completed its first formal cyber vulnerability assessment pursuant to CIP-007-1 R8 eleven months past the required compliance date. The other region also found that the same conduct gave rise to an issue for an affiliate of the entity. NPCC did not consider the affiliate's issue an aggravating factor, as the issues arose from the same conduct.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the cyber vulnerability assessment by its required compliance date, the entity provided examples of actions such as approved purchase orders and statements of work which showed that the elements of the vulnerability assessment were being exercised and documented before the compliant status due date. Further, the entity was not found to be out of compliance with other requirements of CIP-006-1 R1.8.	The entity completed the cyber vulnerability assessment. NPCC verified completion of the mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 5 (NPCC_URE5)	NCRXXXXX	NPCC2011008520	CIP-006-1	R1; R1.1	During a joint compliance audit conducted by NPCC and another region, NPCC determined that the entity had an issue with CIP-006-1 R1. CIP-006-1 R1.1 requires that all Cyber Assets within an Electronic Security Perimeter (ESP) also reside within an identified Physical Security Perimeter (PSP). The entity has two Critical Cyber Assets (CCA) in one PSP within its alternate control center that are connected to a network switch in another separate PSP within the alternate control center. Since all three devices are in the ESP, the network cables that connect these devices are required to be contained within a PSP. However, a section of the two network cables used to connect the CCA to the network switch ran outside the PSPs through the ceiling of a conference room and did not meet the requirement of CIP-006-1 R1.1. The other region also found that the same conduct gave rise to an issue for an affiliate of the entity. NPCC did not consider the affiliate's issue an aggravating factor, as the issues arose from the same conduct.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the network cables that were the cause of this issue were protected by several layers of physical security controls and were not in a public area. The room traversed by the cables was within two additional rings of security and utilized a defense in depth strategy that included fencing, card key access to the building itself, and both exterior and interior camera monitoring. The entire building is limited to employees of the entity and escorted visitors.	The entity completed mitigation activities by running new network cables through the existing conduit that connected the two PSPs. This was performed prior to the completion of the NPCC CIP compliance audit. NPCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 6 (NPCC_URE6)	NCRXXXXX	NPCC201100237	PRC-018-1	R6	The entity self-reported an issue with PRC-018-1 R6. NPCC determined that the entity did not have a formalized corporate maintenance and testing program for all of its disturbance monitoring equipment (DME) as required by the Standard. The review of DME maintenance records failed to demonstrate that all DMEs required by NPCC were covered by the existing process. Furthermore, documented maintenance and testing for those DMEs did not have a standard basis for the intervals. However, the DMEs were tested as part of the entity's facilities' maintenance and testing programs.	NPCC determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though there was no formalized corporate maintenance and testing program for the DMEs required by NPCC, the DMEs have been included as part of the entity's facilities' maintenance and testing programs. Also, the entity has an established relay operation analysis program, in which the DME data is a component of the overall analysis; corrective actions and lessons learned based on DME data is shared with all facilities.	The entity completed mitigation activities, including: 1. established a formalized corporate maintenance and testing program for DMEs including a standardized maintenance and testing program for DMEs; 2. communicated the new program to all responsible personnel and conducted training to facilitate the implementation of the program; and 3. incorporated all DME assets into its automated work control system to ensure implementation and documentation of the maintenance and testing program through a standardized reporting program. NPCC verified completion of the mitigation activities.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001103	CIP-006-3c	R7	The entity self-reported an issue with CIP-006-3c R7 to Reliability*First* and another region. The entity discovered that its access control system's file backup process corrupted data files associated with physical access logs. Specifically, the backup process corrupted approximately 75 hours of stored physical access log data. By recovering some of the corrupted computer data and utilizing video cameras at access points of its Physical Security Perimeters (PSPs), the entity was able to assemble physical entry logs for approximately 70 of the 75 hours of corrupted data. The entity was unable to recover the remaining five hours of corrupt data and therefore could not retain all physical access logs for at least 90 calendar days. Reliability*First* determined that the entity had an issue with the Standard as it did not retain all physical access logs for at least 90 calendar days.	Reliability*First* determined that this remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because during the duration of the remediated issue the access control system operated properly at all PSP access points. Additionally, the entity found no evidence of a cyber attack on its access control system or unauthorized physical intrusion into its PSP. Finally, the five-hour gap in physical access logs is limited to only two PSP access points.	In its Self-Report, the entity states that it reconfigured its access control system's file backup process to preclude any subsequent data loss.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001246	CIP-005-1	R4	During a joint compliance audit conducted by Reliability*First* and another region, Reliability*First* determined that the entity completed its formal cyber vulnerability assessment eleven months past the required compliance date.	Reliability*First* determined that the remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the formal annual cyber vulnerability assessment by the required date, it did complete most of the work required by CIP-005-1 R4.1 through R4.4, including continually reviewing and hardening its Electronic Security Perimeter firewalls. The same conduct gave rise to an issue for an affiliate of the entity in another region but was not considered an aggravating factor.	The entity completed the cyber vulnerability assessment as required by CIP-005-1 R4. The entity completed this mitigation activity as verified at the compliance audit by Reliability*First* .

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	RFC2011001249	CIP-007-1	R8	During a joint compliance audit conducted by Reliability*First* and another region, Reliability*First* determined that the entity completed its formal cyber vulnerability assessment eleven months past the required compliance date.	Reliability*First* determined that the remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the formal annual cyber vulnerability assessment by the required date, it did complete most of the work required by CIP-007-1 R8.1 through R8.4 including continually reviewing and hardening its ESP firewalls. The entity also provided examples of actions, approved purchase orders/statement of work showing that the elements of the vulnerability assessment were being exercised and documented before the compliant status due date. The same conduct gave rise to an issue for an affiliate of the entity in another region but was not considered an aggravating factor.	The entity completed the cyber vulnerability assessment as required by CIP-007-1 R8. The entity completed its mitigation activity as verified at the compliance audit by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001247	CIP-006-1	R1; R1.1	During a joint compliance audit conducted by Reliability*First* and another region, Reliability*First* determined that the entity failed to maintain Critical Cyber Assets (CCAs) within an Electronic Security Perimeter (ESP) within an identified Physical Security Perimeter (PSP). The entity has two CCAs (operator workstations) in one PSP within its alternate control center that are connected to a network switch in another separate PSP within the alternate control center. Since all devices are in the ESP, the network cables that connect these devices are required to be contained within a PSP; however, a section of the two network cables used to connect the CCAs to the network switch ran outside the PSPs through the ceiling of a conference room and did not meet the requirement of CIP-006-1 R1.1.	Reliability*First* determined that the remediated 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 network cables that were the cause of the issue were protected by several layers of physical security controls and were not in a public area. The room traversed by the cables was within two additional rings of security and utilized a defense in depth strategy that included fencing, card key access to the building itself, and has both exterior and interior camera monitoring. The entire building is limited to employees of the entity and escorted visitors. The same conduct gave rise to an issue for an affiliate of the entity in another region but was not considered an aggravating factor.	The entity corrected this issue by running new network cables through an existing conduit that connected the two Physical Security Perimeters (PSPs). This was performed prior to the completion of the compliance audit. The entity completed its mitigation activity as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001248	CIP-006-1	R1; R1.8	During a joint compliance audit conducted by Reliability*First* and another region, Reliability*First* determined that the entity completed its formal cyber vulnerability assessment eleven months past the required compliance date.	Reliability*First* determined that the remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the entity did not complete the cyber vulnerability assessment by the required date, the entity provided examples of actions, approved purchase orders/statement of work showing that the elements of the vulnerability assessment were being exercised and documented before the due date and were not found to be out of compliance with other requirements of CIP-006-1 R1. The same conduct gave rise to an issue for an affiliate of the entity in another region but was not considered an aggravating factor.	The entity completed the cyber vulnerability assessment as required by CIP-006-1 R1. The entity completed its mitigation activity as verified at the compliance audit by Reliability*First.*
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2011001107	FAC-008-1	R1	The entity self-reported an issue with FAC-008-1 R1 to Reliability*First.* The entity identified its gas turbine generators as its most limiting equipment, but did not conduct a review of the associated electrical systems per FAC-008-1 R1. Further, the entity did not formally document a methodology pursuant to FAC-008-1 R1 until past the required date. The entity also did not include terminal equipment in its documented methodology pursuant to FAC-008-1 R1.2.1 until past the required date.	Reliability*First* determined that the remediated 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 entity had identified its gas turbines as the most limiting element at the facility and based all subsequent Facility Ratings accordingly. After identifying and rating all relevant equipment in its facility, the entity determined that it had previously correctly identified the gas turbines as the most limiting element at the facility.	The entity conducted a review of associated electrical systems, documented the Facility Ratings Methodology and revised its methodology to include terminal equipment.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC2011001108	FAC-009-1	R1	The entity self-reported an issue with FAC-009-1 R1 to Reliability*First.* The entity did not document a methodology establishing Facility Ratings for all relevant equipment in its facility until past the required date and therefore did not comply with the FAC-009-1 R1 requirement to have Facility Ratings that are consistent with its methodology.	Reliability*First* determined that the remediated 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 entity had identified its gas turbines as the most limiting element at the facility and based all subsequent Facility Ratings accordingly. After identifying and rating all relevant equipment in its facility, the entity determined that it had previously correctly identified the gas turbines as the most limiting element at the facility.	The entity conducted a review of associated electrical systems, documented the Facility Ratings Methodology and revised its methodology to include terminal equipment.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000390	CIP-003-1	R4; R4.1	During a Self-Certification, SPP RE_URE1 reported that it had an issue with CIP-003-1 R4 because it had not identified, classified, or protected information associated with Critical Cyber Assets (CCAs). Specifically, SPP RE_URE1failed to thoroughly inventory and protect all of its security configuration information such as system configurations, system rule sets, and critical security settings, as required by CIP-003-1 R1.4.	The SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). Although SPP RE_URE1 had not thoroughly inventoried and actively protect its security configuration information, SPP RE_URE1's system rule sets, system configurations, and critical security settings comprising its cyber security information were actually stored on machines within SPP RE_URE1's Electronic Security Perimeter (ESP), which were protected. Additionally, SPP RE_URE1 did provide evidence that it had identified and protected other information associated with its CCAs, including its network topology or similar diagrams, floor plans and computing centers that contain CCAs, equipment layouts of CCAs, disaster recovery plans and incident response plans. Further, SPP RE_URE1 had a written policy in place for the identification, classification and protection of information related to CCAs; however, the policy did not include the specific security configuration information.	To mitigate this issue, SPP RE_URE1 updated its current list of CCAs to ensure that all system security configuration information had been identified, classified and protected from unauthorized access. SPP RE_URE1 modified its existing policy to document the identification, classification and protection of CCA protected information and identified how SPP RE_URE1 personnel will be granted access to this information. The policy also included a change in the management process for incorporating new CCA information or changes to existing CCA information. SPP RE_URE1 trained all affected employees on the new policy. SPP RE_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000398	CIP-005-1	R5; R5.1; R5.3	During a Self-Certification, SPP RE_URE1 reported that it had an issue with CIP-005-1 R5. SPP RE_URE1 reported that it did not have documentation that it had performed an annual review of the documents and procedures referenced in Standard CIP-005 (R5.1). Additionally, because SPP RE_URE1 had not configured all access logs, its access logs were not maintained for a minimum of 90 days as required by R5.3.	The SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). In order for SPP RE_URE1 to be compliant with CIP-005-1 R5, it should have reviewed the documents and procedures referenced in Standard CIP-005 within the required one year time frame. Although SPP RE_URE1 did not have documentation that it had performed any review of its documents and procedures referenced in Standard CIP-005 within the required one year time frame. It is clear that SPP RE_URE1 had reviewed those documents and procedures, as evidenced by the record; however, that review was not within the annual timeframe.	To mitigate this issue, SPP RE_URE1 completed its Mitigation Plans and updated its CIP-005 procedures. Then, SPP RE_URE1 performed an annual review of its CIP-005 documentation. Additionally, SPP RE_URE1 developed a policy to review its CIP-005 documentation at least annually and included requirements to update its CIP-005 documentation to reflect modifications to the network controls within 90 calendar days of a change; retain electronic access logs for at least 90 calendar days; and keep logs related to reportable incidents in accordance with the requirements of CIP-008. SPP RE_URE1 certified that mitigation was complete, and SPP RE verified completion.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201100662	CIP-007-1	R2	SPP RE_URE2 self reported an issue with CIP-007-1 R2. SPP RE_URE2 reported that, while conducting its vulnerability assessment under CIP-007-3 R8, it found that it did not have documented evidence justifying the enabled ports and services on assets within the Electronic Security Perimeter (ESP), which were essential to the normal or emergency operation of SPP RE_URE2's Cyber Assets. Prior to the initial development of SPP RE_URE2's CIP compliance program, SPP RE_URE2's Cyber Assets underwent a "hardening" process where several ports and services were disabled to improve device security. This hardening process was not documented and did not generate sufficient evidence to justify each and every enabled port and service. The vulnerability assessment identified ports and services that were enabled on various devices that were not essential to the normal or emergency operation of SPP RE_URE2's Cyber Assets.	SPP RE 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). SPP RE_URE2 did successfully document that the ports were enabled on specified assets in its previous vulnerability assessment. Furthermore, the ports and services identified in the vulnerability assessment at issue as candidates to be disabled, did not present an obvious threat to the assets as they are operated within an ESP. Prior to the vulnerability assessment at issue, SPP RE_URE2 implemented a system tool that monitors system activity and alerts administrators upon detection of anomalous or suspicious activity. This further reduces the potential impact that the identified problems with CIP-007-1 R2 could cause. Additionally, SPP RE_URE2 has deployed and runs anti-virus and anti-malware software on its Cyber Assets as per CIP-007-1 R4. This reduces the risk of system exploits using viral code recognized by commercial anti-virus solutions. When considering SPP RE_URE2's other protective measures in place, the potential on the BPS was minimal. Following its vulnerability assessment, SPP RE_URE2 began the process of documenting and justifying the enabled ports and services on its Cyber Assets.	Using data from the vulnerability assessment, SPP RE_URE2 has developed a database recording each enabled port and service on every asset inside its ESPs. SPP RE_URE2 has subsequently ensured that this database is aligned with the actual status of each machine. Print outs from this database will be reviewed and signed on a per-machine basis. SPP RE_URE2 also configured its ports and services to conform with the approved ports and services reports. SPP RE_URE2 certified mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP RE_URE3) Calpine Energy Services (CALP)	NCRXXXXX	SPP201100665	CIP-002-1	R4	During a compliance audit, SPP RE determined that SPP RE_URE3 had an issue with CIP-002-1 R4. SPP RE's CIP compliance audit team found that SPP RE_URE3's risk-based assessment methodology (RBAM) was not reviewed or approved by SPP RE_URE3's designated senior manager or a delegate of the senior manager. Instead, a SPP RE_URE3's compliance officer reviewed and approved the RBAM. Because this compliance officer was not also the senior manager, nor was he a delegate of the senior manager, his review and approval of SPP RE_URE3's RBAM did not comply with CIP-002-1 R4.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the issue was related to a documentation error. SPP RE_URE3 did review its RBAM; however, it did not have the correct person approve the RBAM. In addition, the RBAM for the previous year was approved by the correct individual.	SPP RE_URE3 changed the language of its review and approval certification to provide specifically that the RBAM was reviewed and approved separately from the approval of the list of Critical Assets. SPP RE_URE3 certified completion of all mitigating activities.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP RE_URE4) Calpine Corporation (CALPGO)	NCRXXXXX	SPP201100666	CIP-002-1	R4	During a compliance audit, SPP RE determined that SPP RE_URE4 had an issue with CIP-002-1 R4. SPP RE's CIP compliance audit team found that SPP RE_URE4's risk-based assessment methodology (RBAM) was not reviewed or approved by SPP RE_URE4's designated senior manager or a delegate of the senior manager. Instead SPP RE_URE4 compliance officer reviewed and approved the RBAM. Because the chief compliance officer was not also the senior manager, nor was he a delegate of the senior manager, his review and approval of SPP RE_URE4's RBAM did not comply with CIP-002-1 R4.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the issue was related to a documentation error. SPP RE_URE4 did review its RBAM; however, it did not have the correct person approve the RBAM. In addition, the RBAM for the previous year was approved by the correct individual.	SPP RE_URE4 changed the language of its review and approval certification to provide specifically that the RBAM was reviewed and approved separately from the approval of the list of Critical Assets. SPP RE_URE4 certified completion of all mitigating activities.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1)	NCRXXXXX	TRE201100289	FAC-009-1	R1	Texas RE discovered during an audit that the entity did not document how the entity established its Facility Ratings consistent with its Facility Ratings Methodology for the entire compliance period. The entity could not demonstrate that it established Facility Ratings that were consistent with a Facility Ratings Methodology for the entire audit period, as required by this Standard.	Texas RE determined that this issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system (BPS) because the issue was documentation-related. Although the entity's Facility Ratings Methodology did not contain a date, the entity was using regional requirements in determining Facility Ratings and was providing those Ratings to the regional reliability entity as required.	The entity used its Facility Ratings Methodology, which has been addressing the requirements of FAC-008, to develop Facility Ratings, and reports the Ratings to the regional reliability entity. Also, the use of the Facility Rating Methodology is required by the entity's own procedures. Texas RE verified completion of the mitigation activities during the audit.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2) CPS Energy	NCRXXXXX	TRE201000175	CIP-003-1	R1.1	The entity self-reported that its cyber security policy did not address all of the requirements in Standards CIP-002-2 through CIP-009-2, as required by CIP-003-2 R1.1. Texas RE found the policy presented by the entity failed to adequately address the following two requirements: CIP-007-2 R5 and CIP-003-2 R5, as required by this Standard.	This issue did not pose a serious or substantial risk to the bulk power system (BPS) but posed a moderate risk to the BPS. Texas RE determined that the risk was substantially mitigated by the fact that the entity's plan has been in place prior to the mandatory compliance date, and was annually reviewed and updated according to its internal document control procedures, and adequately addressed the vast majority of the requirements in Standards CIP-002-2 thorough CIP-009-2. Yet, a Texas RE review of the entity's cyber security policy revealed that the policy failed to thoroughly address CIP-007-2 R5 and CIP-003-2 R5. Texas RE determined that the entity's more recent version of its cyber security policy is more reflective of the Standards intent, mitigates the issue, and minimizes the risk to the reliability of the BPS.	Texas RE received the entity's updated cyber security plan. The updated policy addresses each applicable CIP standard and requirement. Under each requirement there is a brief description of how the entity meets that requirement. The updated policy mitigates the issue with CIP-003-2 R1.1. The entity revised its policy to mitigate the issue.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE201100382	CIP-005-1	R3	The entity self-reported that it did not address the requirements of this Standard and that it was not technically feasible for the devices (relays that were considered CCAs) at issue to detect and alert attempts for or actual unauthorized accesses to its Electronic Security Perimeter(s), as required by this Standard.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system (BPS) because the devices were in the family of devices that could not support logging. However, the entity controls access to the devices by keycard logging entry and also uses a video camera.	The entity filed a Technical Feasibility Exception (TFE) for this issue. To mitigate the issue, the entity installed a password protected lockbox. Also, maintenance personnel must call security for the password to open the lockbox.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE201100383	CIP-007-1	R4	The entity self-reported that it did not address all requirements of this Standard. The entity stated that it was not technically feasible for the devices at issue (firewall service modules, relays, remote terminal units and switches) to use anti-virus and other malicious software prevention tools to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system (BPS) because the entity restricts administrative access to the devices and does not allow establishing connections with indiscriminate and unknown Internet hosts and devices. Additionally, malware cannot be transferred from one embedded device to another, as the embedded devices are designed not to run any third-party applications.	The entity filed a Technical Feasibility Exception (TFE) for this issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE201000142	CIP-004-1	R4.1	The entity self-reported that it did not adequately perform a review of the list(s) of its personnel who have access to Critical Cyber Assets (CCAs) on quarterly basis. The entity lacked sufficient evidence to demonstrate that reviews of access lists were done comprehensively and timely by all affected operational organizations. The affected organizations stated that they had timely performed the reviews, but lacked sufficient evidence to demonstrate satisfactory compliance with this Standard.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system (BPS) because this was a documentation issue, which was mitigated by the entity's ongoing security program and its additional methods of determining misuse and threats to its systems, which include card-key access, security cards and/or video surveillance at access locations.	The entity completed its Mitigation Plan, which included training and spot checking of the entity's personnel compliance with the newly revised policies and procedures. The entity also installed and began using a new tracking software to further ensure compliance.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE201000145	CIP-007-1	R6	The entity self-reported that its Critical Cyber Asset (CCA) systems all provide for sending automated alerts to appropriate personnel when Cyber Security Incidents occur and that these alerts are sent to its employees. However, the entity determined that it has not adequately documented the fact that such log reviews have taken place and, as such, did not maintain records documenting review of logs. Based on the record, Texas RE determined that there was an issue with this Standard.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because this is a documentation issue, which was mitigated by the entity's ongoing security program and its other methods of determining misuse and threats to its systems the entity was maintaining and reviewing logs of system events. Texas RE determined that this was a documentation issue because the entity had not adequately document the fact that log reviews were being done.	The entity completed its Mitigation Plan, which included training and spot checking of its personnel's compliance with the newly revised policies and procedures to eliminate a reoccurrence of this issue. The entity also installed and began using new tracking software to further insure compliance. The entity also uses automated reports and quarterly reviews, which are documented on a form document.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (Texas RE_URE4)	NCRXXXXX	TRE201000248	PRC-005-1	R1.1	Texas RE_URE4 self-reported that it did not have adequate bases for its Protection System maintenance and testing program. Texas RE determined that the bases for the test intervals for relay testing, batteries, instrument transformers and DC control circuitry were missing or inadequate, as required by PRC-005-1 R1.	Texas RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Texas RE_URE4 was performing Protection System maintenance and testing at intervals that were the same as or shorter than those specified by the NERC-published document *Protection System Maintenance - A Technical Reference Sep. 2007* . Therefore, Texas RE determined that the absence or inadequacy of suitable bases was a documentation issue.	Texas RE_URE4 mitigated this issue by implementing a revised maintenance and testing procedure, which included adequate bases for the intervals specified for its Protection System. Texas RE verified completion of the mitigation.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 5 (Texas RE_URE5)	NCRXXXXX	TRE201100138	CIP-007-1	R5.1.2	Texas RE_URE5 self-reported noncompliance with CIP-007-1 R5. Based on the Self-Report, Texas RE determined that while preparing to transition to a new generation management system (GMS) in accordance with ERCOT ISO's transition to Nodal Market, legacy Texas RE_URE5's GMS was not capable of complying with R5.1.2. The legacy GMS system was not configured to track and log the shared accounts running on it at any given time. Texas RE_URE5 was notified, by a consultant, that the legacy GMS was infeasible and it would take longer to update the older system to comply with CIP-007 R5.1.2 then to begin using the new GMS with the new Nodal Market.	Texas RE determined this issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because during the short duration of noncompliance, Texas RE_URE5 worked to minimize any changes to its legacy GMS. Any changes that were made to this system were being tracked on a day-to-day basis. Furthermore, at each generation facility, a control room is in place to monitor the status of the plant in real time. Were a signal to arise from the GMS to indicate an anomaly (*i.e.* something that is not in line with standard operating metrics), the facility is removed from automatic voltage control until the anomaly is rectified. Lastly, Texas RE_URE5 stated that all anti-virus definitions are current, that all employees requiring physical and cyber access have completed background checks, and that these employees have completed training and are approved for the appropriate access.	Texas RE_URE5 mitigated this issue by acquiring the necessary equipment, installing the new network and hardware, implementing a new management system and initiating all required access control, logging and monitoring controls. The issue was mitigated once the transition to the new Nodal Market was completed and the new management system were in place.

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 6 (Texas RE_URE6) City of Fredericksburg	NCRXXXXX	TRE201100295	CIP-001-1	R1	In an audit, Texas RE found that Texas RE_URE6's sabotage awareness documents did not contain any procedures for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting large portions of the Interconnection.	Texas RE determined this issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because the issue period was short, Texas RE_URE6 was included in the county's emergency management plan, the entity is small and the number of its operating personnel is also limited. During the period when Texas RE_URE6 was not fully compliant with CIP-001-1 R1, it was included in the established county's emergency management plan for the duration of noncompliance. Portions of the emergency management plan relate to responses to sabotage events and it is partially compliant with CIP-001-1.	Texas RE_URE6 mitigated this issue by updating its sabotage awareness procedure and addressing the requirements of CIP-001-1 R1. A Mitigation Plan was submitted as complete.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2011009019	MOD-019-0.1	R1	WECC_URE1 did not respond to a request to provide forecasts of interruptible demands and Direct Control Load Management (DCLM) to WECC. Due to an internal communication and administrative oversight, WECC_URE1 did not respond to the request. WECC_URE1 did provide the forecasts of interruptible demands and DCLM for the prior year.	WECC_URE1 does not have any interruptible demands nor DCLM programs, therefore the response would have been null had WECC_URE1 responded timely. For these reasons, WECC determined these issues posed minimal and not serious or substantial risk to the bulk power system.	Upon discovery of the issue, WECC_URE1 sent a request to ask if the oversight required rectification. The request included a deadline, after which the assumption would be that WECC_URE1 had no MW participating in any of its programs. Since WECC_URE1 would have shown zero MW, the analyses prepared properly reflected what WECC_URE1 would have submitted. To mitigate this issue, which was caused by an oversight within internal communications, WECC_URE1 clarified the roles and responsibilities for personnel and established redundancy in the communication links. 1. WECC_URE1's utility director is included as a recipient for all correspondence regarding NERC Reliability Standards matters. 2. WECC_URE1 finalized an internal procedure governing loads and resources data preparation. 3. WECC_URE1 consulted and confirmed its respective responsibilities with respect to NERC compliance matters and provided training to all relevant staff members. 4. As part of the internal compliance program a compliance calendar was put in place. The compliance calendar includes all known compliance dates and includes both alert and tracking capabilities. Note: A single incident resulted in the issue of three NERC Reliability Standards: MOD-019-0.1 R1, MOD-020-0 R1 and MOD-021-0.1 R1. While the facts of each issue are different, the mitigation measures are identical for each issue.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2011009020	MOD-020-0	R1	WECC_URE1 did not respond to a request to provide forecasts of interruptible demands and Direct Control Load Management (DCLM) to WECC. Due to an internal communication and administrative oversight, WECC_URE1 did not respond to the request. WECC_URE1 did provide the forecasts of interruptible demands and DCLM for the prior year.	WECC_URE1 does not have any interruptible demands nor DCLM programs, therefore the response would have been null had WECC_URE1 responded timely. For these reasons, WECC determined these issues posed minimal and not serious or substantial risk to the bulk power system.	Upon discovery of the issue, WECC_URE1 sent a request to ask if the oversight required rectification. The request included a deadline, after which the assumption would be that WECC_URE1 had no MW participating in any of its programs. Since WECC_URE1 would have shown zero MW, the analyses prepared properly reflected what WECC_URE1 would have submitted. To mitigate this issue, which was caused by an oversight within internal communications,WECC_URE1 clarified the roles and responsibilities for personnel and established redundancy in the communication links. 1. WECC_URE1's utility director is included as a recipient for all correspondence regarding NERC Reliability Standards matters. 2. WECC_URE1 finalized an internal procedure governing loads and resources data preparation. 3. WECC_URE1 consulted and confirmed its respective responsibilities with respect to NERC compliance matters and provided training to all relevant staff members. 4. As part of the internal compliance program a compliance calendar was put in place. The compliance calendar includes all known compliance dates and includes both alert and tracking capabilities. Note: A single incident resulted in the issue of three NERC Reliability Standards: MOD-019-0.1 R1, MOD-020-0 R1 and MOD-021-0.1 R1. While the facts of each issue are different, the mitigation measures are identical for each issue.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2011009021	MOD-021-0.1	R3	WECC_URE1 did not respond to a request to provide documentation on the treatment of its Demand-Side Management programs to WECC. Due to an internal communication and administrative oversight, WECC_URE1 did not respond to the request.	WECC_URE1 does not have any interruptible demands nor DCLM programs, therefore the response would have been null had WECC_URE1 responded timely. For these reasons, WECC determined these issues posed minimal and not serious or substantial risk to the bulk power system.	Upon discovery of the issue, WECC_URE1 sent a request to ask if the oversight required rectification. The request included a deadline, after which the assumption would be that WECC_URE1 had no MW participating in any of its programs. Since WECC_URE1 would have shown zero MW, the analyses prepared properly reflected what WECC_URE1 would have submitted. To mitigate this issue, which was caused by an oversight within internal communications, WECC_URE1 clarified the roles and responsibilities for personnel and established redundancy in the communication links. 1. WECC_URE1's utility director is included as a recipient for all correspondence regarding NERC Reliability Standards matters. 2. WECC_URE1 finalized an internal procedure governing loads and resources data preparation. 3. WECC_URE1 consulted and confirmed its respective responsibilities with respect to NERC compliance matters and provided training to all relevant staff members. 4. As part of the internal compliance program a compliance calendar was put in place. The compliance calendar includes all known compliance dates and includes both alert and tracking capabilities. Note: A single incident resulted in the issue of three NERC Reliability Standards: MOD-019-0.1 R1, MOD-020-0 R1 and MOD-021-0.1 R1. While the facts of each issue are different, the mitigation measures are identical for each issue.

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	WECC2011008665	VAR-501-WECC-1	R1	For approximately 22 hours, one of WECC_URE2's units operated with the Power System Stabilizers (PSS) not in service. The unit operated with the PSS in service less than 98% (but greater than 95%) of the generator's on-time service for the 4th quarter. WECC_URE2 discovered and corrected the PSS status on the same day it occurred.	WECC determined this issue posed a minimal risk and not a serious or substantial risk to the bulk power system. While failure to operate voltage regulators without the PSS in service may reduce the margins of stable operation of the generating facility during transient conditions, in this case the unit operated with its PSS in service for the majority of the calendar quarter, reducing the probability of dynamic instability, thus reducing the probability of an unnecessary loss of a facility during a transient event. In this case, the automatic voltage regulators protected the unit by ensuring the generator could respond to changes in voltage. WECC_URE2 operated its remaining generators with the PSS in service, with the automatic voltage regulators in voltage control mode, set to respond effectively to voltage deviations. Further, the issue represented a small amount of WECC_URE2's total generation and an even smaller amount of the total generating capacity available to WECC_URE2.	WECC_URE2 returned the PSS to service and trained its operators on PSS display information.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC201102824	CIP-007-1	R4	WECC_URE3 performed an in-depth inventory of the Cyber Assets contained within the Electronic Security Perimeters (ESPs) for its substations. As a result of that inventory, WECC_URE3 discovered Cyber Assets that required a Technical Feasibility Exception (TFE) for CIP-007-1 R4 because they lacked a capability for the installation of malicious software prevention tools. WECC_URE3 self-reported an issue with the CIP Standards arising from WECC_URE3's failure to timely submit TFE requests in accordance with NERC procedures. The Self-Report referenced all identified TFEs that should have been filed as of that point. WECC_URE3's TFE requests were submitted approximately 16 to 20 months late. Specifically, WECC_URE3 submitted 37 late TFE requests for CIP-007-1 R4. WECC reviewed and accepted the TFE and determined it is technically infeasible for WECC_URE3 to comply with the Standard for the devices associated with the TFE Identification number.	All devices in scope are located in Physical Security Perimeters (PSPs) and ESPs and thus afforded the protections of CIP-005 and CIP-006. Additionally, all individuals with access to the devices have a valid personnel risk assessment and training. For these reasons, WECC 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.	WECC_URE3 filed the TFEs with WECC and WECC approved the Part A and Part B TFE. WECC_URE3 has implemented an intrusion detection system (IDS) which monitors all network traffic and sends automated alerts upon detecting suspicious traffic. All devices in scope are located in PSPs and ESPs and thus afforded the protections of CIP-005 and CIP-006. Additionally, all individuals with access to the devices have a valid personnel risk assessment and training.

Document Content(s)