Federal Energy Regulatory Commission
Washington, D.C. 20426

December 22, 2021

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

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDefenseBook@gmail.com

Dear Mr. Mabee:

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

By letter dated December 9, 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. RC12-10, 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 RC12-10.

With respect to the remaining identities of UREs contained in RC12-10, before making a determination as to whether this information is appropriate for release under

[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.

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-10 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 13:00:25 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

March 30, 2012

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

RC12-10

East Mississippi Electric Power Association (EMEPA)-.pdf page 22

Nelson Industrial Steam Company (NISCO)-.pdf page 23

City of San Marcos (COSM)-.pdf page 23

GIM Channelview Cogeneration, LLC (CVC)-.pdf page 24

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 12 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 21 possible violations[5] of 9 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 21 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

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

enforcement processes for occurrences that posed 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 certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, spot check, random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

[6] *See North American Electric Reliability Corporation*, 138 FERC ¶ 61,193 (2012) ("March 15, 2012 CEI Order"); *see also North American Electric Reliability Standards Development and NERC and Regional Entity Enforcement*, 132 FERC ¶ 61,217 at P.218 (2010)(encouraging streamlined administrative processes aligned with the significance of the subject violations).
[7] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Resolution[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,[9] NERC Enforcement staff under delegated authority from the NERC BOTCC, approved the FFT based upon its findings and determinations, as well as its review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the remediated issues.

Notice of Completion of Enforcement Action

In accordance with section 5.10 of the CMEP, and the Commission's March 15, 2012 CEI Order, provided that the Commission has not issued a notice of review of a specific matter included in this filing, notice is hereby provided that, sixty-one days after the date of this filing, enforcement action is complete with respect to all remediated issues included herein and any related data holds are released only as to that particular remediated issue.

Pursuant to the Commission order referenced above, both the Commission and NERC retain the discretion to review a remediated issue after the above referenced sixty-day period if it finds that FFT treatment was obtained based on a material misrepresentation of the facts underlying the FFT matter. Moreover, to the extent that it is subsequently determined that the mitigation activities described herein were not completed, the failure to remediate the issue will be treated as a continuing possible violation of a Reliability Standard requirement that is not eligible for FFT treatment.

Request for Confidential Treatment of Certain Attachments

Certain portions of Attachment A include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain

[8] *See* 18 C.F.R § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation,* 132 FERC ¶ 61,182 (2010).

Reliability Standard possible violations and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the information in the attached documents is deemed "confidential" by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be included as Part of this FFT Informational Filing

The attachments to be included as part of this FFT Informational Filing are the following documents and material:

a) Find Fix and Track Report Spreadsheet, included as Attachment A; and

b) Additions to the service list, included as Attachment B.

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001 (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 MARCH 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 SERC:

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

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

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

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

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

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
March 30, 2012

Take notice that on March 30, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding twelve (12) 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
Reliability*First* Corporation (Reliability*First)*	NRG Rockford LLC (NRG Rockford)	NCR06025	RFC2011001098	PRC-005-1	R2; R2.1	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit of NRG Rockford (Compliance Audit) and discovered that NRG Rockford, as a Generator Owner, had an issue with PRC-005-1 R2.1. Although NRG Rockford's generation Protection System maintenance and testing program (Program) included a two-year interval for associated communication systems, NRG Rockford did not provide Reliability*First* with evidence that it tested its associated communication systems prior to May 2, 2011. NRG Rockford's communication systems at issue are associated with four SEL-321 relays at the point of interconnection. Since NRG Rockford could not provide Reliability*First* with evidence that it tested its associated communication systems within two-year intervals, Reliability*First* could not verify that the entity maintained and tested its associated communication systems according to its Program.	In light of the nature of the remediated issue, offset by the following mitigating factors, 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). The risk to the reliability of the BPS was mitigated by the following factors. The remediated issue is primarily a documentation error because NRG Rockford was continually monitoring their associated communication systems, but did not provide Reliability*First* with evidence demonstrating that fact during the Compliance Audit. NRG Rockford employs continuous monitoring and self-testing features on its associated communication systems and has done so since June 18, 2007. Specifically, four relays at NRG Rockford's energy center that tie to relays at the Commonwealth Edison Company's Sabrooke station continually test the two communication lines between the two locations. NRG Rockford tests the associated communication systems approximately 60 times per second using a protocol called Mirrored Bits, and alarms are triggered in the event that 1) a relay is disabled; 2) the Mirrored Bits protocol is not enabled; 3) data is received in error; or 4) no message is received within the time that three messages are sent. NRG Rockford performed manual maintenance and testing of the associated communication systems on May 2, 2011, which simply confirmed the results of the automatic testing which occurs 60 times per second. Finally, no alarms sounded for the associated communications systems at NRG Rockford's energy center for the duration of the remediated issue.	During the Compliance Audit, NRG Rockford submitted evidence that it performed manual tests on its associated communication systems on May 2, 2011. Reliability*First* determined that this evidence demonstrated that NRG Rockford tested and maintained its associated communication systems.
Reliability*First* Corporation (Reliability*First)*	NRG Rockford II LLC (NRG Rockford II)	NCR06024	RFC2011001101	PRC-005-1	R2; R2.1	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit of NRG Rockford II (Compliance Audit) and discovered that NRG Rockford II, as a Generator Owner, had an issue with PRC-005-1 R2.1. Although the NRG Rockford II's generation Protection System maintenance and testing program (Program) included a two-year interval for associated communication systems, NRG Rockford II did not provide Reliability*First* with evidence that it tested its associated communication systems prior to May 2, 2011. NRG Rockford II's communication systems at issue are associated with four SEL-321 relays at the point of interconnection. Since NRG Rockford II could not provide Reliability*First* with evidence that it tested its associated communication systems within two-year intervals, Reliability*First* could not verify that NRG Rockford II maintained and tested its associated communication systems according to its Program.	In light of the nature of the remediated issue, offset by the following mitigating factors, 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). The risk to the reliability of the BPS was mitigated by the following factors. The remediated issue is primarily a documentation error because NRG Rockford II was continually monitoring its associated communication systems, but did not provide Reliability*First* with evidence demonstrating that fact during the Compliance Audit. NRG Rockford II employs continuous monitoring and self-testing features on its associated communication systems and has done so since June 18, 2007. Specifically, four relays at NRG Rockford II's energy center that tie to relays at the Commonwealth Edison Company's Sabrooke station continually test the two communication lines between the two locations. NRG Rockford II tests the associated communication systems approximately 60 times per second using a protocol called Mirrored Bits, and alarms are triggered in the event that 1) a relay is disabled; 2) the Mirrored Bits protocol is not enabled; 3) data is received in error; or 4) no message is received within the time that three messages are sent. NRG Rockford II performed manual maintenance and testing of the associated communication systems on May 2, 2011, which simply confirmed the results of the automatic testing which occurs 60 times per second. Finally, no alarms sounded for the associated communications systems at NRG Rockford II's energy center for the duration of the remediated issue.	During the Compliance Audit, NRG Rockford II submitted evidence that it performed manual tests on its associated communication systems on May 2, 2011. Reliability*First* determined that this evidence demonstrated that NRG Rockford II tested and maintained its associated communication systems.

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*)	Duquesne Light Company (Duquesne)	NCR00762	RFC2011001214	PRC-005-1	R2	From October 17, 2011 through October 21, 2011, Reliability*First* conducted a compliance audit of Duquesne (Compliance Audit) and discovered that Duquesne, as a Distribution Provider and Transmission Owner, had an issue with PRC-005-1 R2. Duquesne could provide evidence of relay testing, but could not provide maintenance and testing records for current transformers (CTs), potential transformers (PTs), DC control circuitry and associated communication systems. Prior to 2011, Duquesne used procedures that required field personnel to perform and complete maintenance and testing for all CTs, PTs, DC control circuitry and associated communication systems before changing the relay work order status to "complete." Only upon completion of all of the steps in the work order, including the testing of CTs, PTs, DC control circuitry and associated communication systems, would the work order be completed, although Duquesne did not explicitly document those testing steps. However, beginning in 2010, Duquesne modified its work order forms to provide higher quality evidence, and Duquesne's maintenance records now include a specific checklist for testing of CTs, PTs, DC control circuitry and associated communication systems.	In light of the nature of the issue, offset by the following mitigating factors, 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). The risk posed to the BPS was mitigated by the fact that Duquesne maintained and tested all Protection System devices at issue, and that the issue was limited to the quality of its testing documentation. Additionally, Duquesne uses voltage alarms to detect PT problems, and supervisory control and data acquisition (SCADA) system tools to identify CT problems. Duquesne's primary communication system for its Protection System is a synchronous optical networking system, which features self-healing characteristics and real-time health alarming. During the time period of this issue, four instances of substation alarms occurred, which resulted in the automatic generation of a work order to investigate PT sensing circuitry under-voltage conditions. SCADA system tools also identified one instance of a CT problem. Duquesne successfully addressed all five issues via the work orders, making repairs as needed.	During the Compliance Audit, Duquesne provided evidence that it updated its transmission Protection System maintenance and testing program, and provided a new checklist template utilized to document its maintenance and testing for CTs, PTs, DC control circuitry and associated communication systems. Reliability*First* verified that Duquesne mitigated the remediated issue.
Southwest Power Pool Regional Entity (SPP RE)	Eastman Cogeneration Limited Partnership (Eastman)	NCR01092	SPP201000294	FAC-008-1	R1	During a June 8, 2010 through June 9, 2010 compliance audit, SPP RE determined that Eastman had an issue with NERC Standard FAC-008-1 R1. Eastman's Facility Rating Methodology (Methodology), which was implemented on May 4, 2010, did not identify all of the required elements and methods for determining Facility Ratings, as required by the Standard. Eastman's Methodology stated that Eastman would use a model based on the variation in the facility's host load and ambient conditions to calculate its Facility Rating. But its Methodology failed to include the scope of equipment comprising its generating facilities in order to determine the most limiting element and to develop a Facility Rating. Furthermore, it failed to state the method for determining ratings, such as failing to include manufacturer ratings, design criteria and operation limitations. Additionally, Eastman could not provide any Methodology for the period prior to May 4, 2010.	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). Although Eastman had not initially identified the most limiting element within its generation Facility using its Methodology, Eastman had determined the generating capacity of its co-generation facility by using a computer model of the facility. Eastman's generating capacity was determined based upon the steam load supplied to its host, a chemical plant, which receives most of the energy produced by Eastman's facility. The excess capacity not used by the host is supplied to the BPS. Eastman has been using its computer model since 2004 to determine its next-day generating capacity of its facility. Additionally, in implementing its revised Methodology, Eastman's computer model was validated and no changes were made to the existing model. The model identified the facility generator as the most limiting element.	Eastman initiated an engineering study to determine the most limiting element and develop a Methodology. The scope of the equipment in the study included the generator step-up transformers, relay protective devices, disconnect switches, line switches, breakers, current transformer ratios, standalone current transformers, solid bus strung bus jumpers/risers and relay settings. The Facility Rating Methodology also included the method used in determining the Facility Rating and considered manufacturer ratings, design criteria and operating limitation of the elements that comprise the generating facility. Eastman certified completion of these mitigation activities and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Eastman Cogeneration Limited Partnership (Eastman)	NCR01092	SPP201000295	FAC-009-1	R1	During a June 8, 2010 through June 9, 2010 compliance audit, SPP RE determined that Eastman had an issue with NERC Standard FAC-009-1 R1. Eastman had not established a capacity rating for its generating facility using a Facility Rating Methodology (Methodology) that met the requirements of FAC-008-1. Instead, Eastman used a computer model to establish, on a daily basis, its generating capacity based upon the forecast steam load required from its host. When asked to provide evidence of a Facility Rating, Eastman provided only a forecasted energy output of its generating facility. This data did not include all of the elements that comprised the generating facility and, as a result, Eastman could not demonstrate that its generating Facility Rating was based on the most limiting element that comprises the generating facility.	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). Although Eastman had not initially identified the most limiting element in its generation Facility Rating using its Methodology, Eastman had determined the generating capacity of its generating facility by using a computer model of the generating facility. Eastman's generating capacity was determined based upon the steam load supplied to its host, a chemical plant, which receives most of the energy produced by Eastman's facility. The excess capacity not used by the host is supplied to the BPS. Eastman has been using its computer model since 2004 to determine its next-day generating capacity of its facility. Additionally, in implementing its revised Methodology, Eastman's computer model was validated and no changes were made to the existing model. The model identified the facility generator as the most limiting element.	The engineering study and Methodology completed for FAC-008-1 was used to establish a Facility Rating. Eastman certified completion of these mitigation activities.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	Eastman Cogeneration Limited Partnership (Eastman)	NCR01092	SPP201000296	FAC-009-1	R2	During a June 8, 2010 through June 9, 2010 compliance audit, SPP RE determined that Eastman had an issue with NERC Standard FAC-009-1 R2. Eastman could not provide evidence that the Facility Ratings Eastman provided to its Reliability Coordinator (RC), Transmission Operator (TOP), Transmission Planner (TP) and Planning Authority (PA) were derived from a compliant Rating Methodology, as required by FAC-009-1 R2.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although Eastman did not have Facility Rating based upon a compliant Facility Ratings Methodology to provide to its RC, TOP, TP and PA, Eastman had been determining the generating capacity of its co-generation facility by using a computer model of the facility. In addition, during the time of the issue, Eastman was providing its generating capacity of the generating facility to its TOP and BA, American Electric Power (AEP), which is also serving as Eastman's TP. AEP provided these results to SPP, Inc., Eastman's RC and PA. Eastman's generating capacity was determined based upon the steam load supplied to its host, a chemical plant, which receives most of the energy produced by Eastman's facility. The excess capacity not used by the host is supplied to the BPS. Eastman has been using its computer model since 2004 to determine its next-day generating capacity of its facility. Additionally, in implementing its revised Methodology, Eastman's computer model was validated and no changes were made to the existing model. The model identified the facility generator as the most limiting element.	The Facility Rating established using the Facility Rating Methodology has been provided to associated RCs, PAs, TPs and TOPs. Eastman certified 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
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007267	CIP-004-3	R2	FRCC_URE1 self-reported an issue with CIP-004-3 R2. FRCC_URE1 did not provide the proper training to two employees granted access to Critical Cyber Assets. Specifically, two long-term employees were granted NERC CIP access without having completed the proper NERC training. The first employee did not complete the annual required training and upon discovery five months later, the annual training was completed promptly. This employee had successfully completed 2009 and 2010 annual training, but his 2011 annual training was delayed by five months and six days. The second employee was inadvertently given access and was not trained prior to having access. His excess access privileges to NERC CIP Physical Security Perimeters (PSP) were revoked within six days. He was not aware that he had access nor did he exercise access during these six days.	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 employees involved were long-term FRCC_URE1 personnel with satisfactory personnel risk assessments (PRAs). For the first employee, the annual training was delayed by five months, whereupon he completed the training with satisfactory results. With respect to the second employee, an incorrect badge was issued to a new employee who was not authorized for access to the secured PSP. This employee's access privileges to NERC CIP PSPs were revoked within six days. He was not aware that he had access nor did he exercise access during these six days. Although FRCC_URE1 has violated this Standard previously, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation appropriately. The systems that FRCC_URE1 put in place to prevent recurrence of the prior violation were implemented for its transmission-related functions. The generation-related functions are managed separately and are the subject of the instant remediated issues.	With respect to the first employee, FRCC_URE1 provided the required training, which the employee completed with satisfactory results. FRCC_URE1's information security department corrected the improper access for the second employee and conducted a coaching session to re-emphasize the importance of following established procedures with staff responsible for processing card keys. Additionally, FRCC_URE1 modified the desk level procedure and trained its employee groups involved in granting physical and cyber access to reinforce the importance of following access procedures. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007978	CIP-004-3	R2	FRCC_URE1 self-reported an issue with CIP-004-3 R2. FRCC_URE1 allowed access to Critical Cyber Assets (CCA) for two contractors who were not trained as per FRCC_URE1's training program, as required by the Standard. These contractors were employees of a trusted vendor with a service level agreement for tuning and maintaining generating plant equipment. Access was granted on two occasions for very short durations (1 day and 3 days) and access and activity was monitored by generating plant operating personnel.	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 two contractors were employees of a very large generating plant turbine equipment manufacturer, were authorized for turbine tuning, and have experience and sufficient training to handle the plant equipment. The vendor is responsible for plant equipment support and is under an obligation to maintain the plant equipment. In all instances, the access was controlled and all activities, including modifications, were performed in complete consultation with and observation by the plant operations staff. Although FRCC_URE1 has violated this Standard previously, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation appropriately. The systems that FRCC_URE1 put in place to prevent recurrence of the prior violation were implemented for its transmission-related functions. The generation-related functions are managed separately and are the subject of the instant remediated issues.	FRCC_URE1 validated cyber security training for all access granted through the use of a vendor service request and on-boarding process. FRCC_URE1 also reviewed all vendor contractors who have performed remote access vendor support. Additionally, FRCC_URE1 updated and communicated procedures to ensure that vendor contractors providing support follow the full on-boarding process for contractors and have a completed annual cyber security training. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007929	CIP-006-1	R1 (R1.1)	FRCC_URE1 self-reported an issue with CIP-006-1 R1. FRCC_URE1 failed to maintain a complete "six-wall" perimeter for five identified Physical Security Perimeters (PSPs) and failed to submit a TFE request, as required by the Standard. A review determined that the openings at issue were not easily accessible, as they were obstructed by carpets, furniture and plant equipment. All of the openings were located in ceilings or floors and FRCC_URE1 self-reported and corrected these after receiving guidance from NERC and FRCC that any opening greater than 96 square inches is an access point.	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 a review determined that the openings at issue were not easily accessible, as they were obstructed by carpets, furniture and plant equipments.	To correct the issues at the control center, FRCC_URE1 installed sub-floor panels and extended the wall above the ceiling to the roof decks. Additionally, FRCC_URE1 updated the physical security plan to include the more restrictive criteria and documented changes in the change log as per the 30-day requirement. Further, the facility services developed procedures for checking the adequacy of the "six-wall" perimeters for PSPs in the future. The procedures consist of a checklist to help ensure application of the NERC and FRCC guidance criteria. FRCC verified the 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
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201000406	CIP-006-2	R1 (R1.2)	FRCC_URE1 self-reported an issue with CIP-006-2 R1. FRCC_URE1 documented, implemented, and maintained a physical security plan, approved by the senior manager or delegate. However, FRCC_URE1 failed to identify one physical access point through the Physical Security Perimeter (PSP) and failed to identify the measures to control entry at this access point. Although the physical access point was not documented, most appropriate security controls were effective. The access point in question was for a HVAC maintenance access point in a ceiling inside the PSP. The HVAC access had an unlocked latch. The latch was locked and the issue corrected 461 days after the issue began.	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 access point and access control methods were not documented for one access point, the access point was in a secured facility and was under constant observation. This facility is also secured with a 12-foot fence, is monitored by armed security guards at the gate, and is monitored periodically by a roving armed security guard. Access to the facility is only allowed for appropriate individuals based on need and justification and all individuals are screened at the gates.	FRCC_URE1 completed the following mitigation activities: (1) Installed a compliance CIP-controlled lock at the attic hatchway access point and created control procedure for access and use of a key prior to entry. The keys to these controlled locks are maintained in a secure location; (2) Enhanced facility services internal procedure regarding construction at applicable CIP-designated locations to prevent future occurrence of the construction-related hatch issue; (3) Updated the PSP drawings to include the hatch access and applicable access controls; (4) Conducted refresher training for facility services and Corporate Security employees; (5) Completed a one-time physical inspection of all "six-wall" perimeters at all PSP locations above and beyond the annual physical walkthrough, and corrected any exceptions to the physical security plan identified as a result of the review; and (6) Updated the physical security plan and Physical Perimeters Verification Form for verification of annual walkthrough. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007971	CIP-006-2	R2	FRCC_URE1 self-reported an issue with CIP-006-2 R2. FRCC_URE1 failed to identify one of the Cyber Assets used in the authorization and logging of access to the Physical Security Perimeter (PSP) for a generating unit identified as a Critical Asset with designated PSPs. FRCC determined that one of the physical access controllers was not documented but was appropriately protected as required by CIP-006 R2.2. Additionally, certain TFEs were submitted late for the requirements where it was technically infeasible to maintain strict compliance. TFEs were accepted by the region.	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 the result of a lack of documentation. The subject physical access controller was afforded all the required security controls of CIP-006-2 R2.2 that were technically feasible and only lacked submission of TFEs for requirements with technical limitation for the subject device. All comparable compensating and mitigating measures were in effect from the time of commissioning of the device, including firewall protection, procedural controls for password complexity and annual change, and procedural controls for malware protection and patching. A TFE was submitted late and accepted by the FRCC.	FRCC_URE1 reviewed the physical access control system and ensured that all cardkey control panels that control access for PSPs appear on the Cyber Asset list. FRCC_URE1 submitted appropriate existing cardkey TFEs for correct asset count. FRCC verified completion of the mitigation activities.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008072	CIP-006-3c	R1 (R1.6)	FRCC_URE1 self-reported an issue with CIP-006 R1.6. On one occasion, one visitor was allowed access to a designated Physical Security Perimeter (PSP) and FRCC_URE1 failed to document the departure time and escort name. FRCC_URE1 has self-reported even though these logs are outside the 90-day log retention window as required by CIP standards. FRCC_URE1 further provided corroborating evidence and supporting attestation demonstrating the escort's identity and departure time. The evidence demonstrated that the visitor was continuously escorted during his brief stay in the PSP.	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 this was an isolated event which was the result of lack of complete documentation. The subject visitor was continuously escorted by authorized personnel and stayed in the PSP for a very short duration.	FRCC_URE1 completed a review of PSP visitor records to determine whether there were any additional occurrences by reviewing electronic and manual logs. Since no additional instances were found, FRCC_URE1 trained identified escorts regarding the requirement to complete the visitor log in full. FRCC_URE1 also issued awareness reminders to affected personnel reinforcing its visitor escort procedures. FRCC 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
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011007968	CIP-007-1	R4 (R4.2)	FRCC_URE1 self-reported an issue with CIP-007-1 R4. For a period of approximately two and a half years, FRCC_URE1 failed to implement its anti-virus update procedure for testing and installing anti-virus signatures for various corporate and generating Cyber Assets that were required to comply with the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all signatures were released from reliable vendors involving a thorough evaluation of the anti-virus signatures. All signatures other than the those released on weekends were tested using days of test data. Corporate system updates preceded the updates for the weekend signatures, limiting any significant risk to the Critical Cyber Assets (CCA). The corporate Cyber Assets were dedicated for administration of physical access controllers and the risk was minimal, as any adverse impact to these systems as a result of a malware signature update could not have impacted the BPS control and monitoring function. Physical access controls would continue to operate effectively without the administrative workstations, which are utilized to modify and update configurations only.	FRCC_URE1 resolved the anti-virus signature propagation delay for the Cyber Assets by modifying the application configuration. For the assets where configuring delay was not technically feasible with the current anti-virus product, FRCC_URE1 upgraded the anti-virus application to a different product that allowed for such propagation delay. FRCC_URE1 also updated the procedure documents to reflect the new configuration. FRCC verified completion of the mitigation activities.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007268	CIP-007-1	R3	NPCC_URE1 self-reported an issue with CIP-007-1 R3. NPCC_URE1 has a documented security patch management program (CIP Security Patch Management Program). NPCC_URE1's program did not include the specific database associated with the energy management system (EMS) for a seven-month period.	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 NPCC_URE1 had already been analyzing and reviewing the patches at issue in accordance with the CIP Security Patch Management Program, despite the fact that the program did not specifically include it.	NPCC_URE1 provided documentation that the database was added to the corporate security patch management program. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011007274	CIP-005-1	R2; R2.6	NPCC_URE1 self-reported an issue with CIP-005-1 R2.6. NPCC_URE1 self-reported that, for a 17-month period, all firewalls associated with the three corporate Electronic Security Perimeters (ESPs) did not display the appropriate use banner upon interactive access attempts, as required by the Standard.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE1 has account administration controls in effect and strict physical security controls in place that limited access to certain users.	NPCC_URE1 provided documentation that the appropriate banners were added to all firewalls. The mitigation activity was verified complete by NPCC.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) East Mississippi Electric Power Association (EMEPA)	NCRXXXXX	SERC2012009645	CIP-003-2	R2	SERC_URE1 self-certified a possible issue with CIP-003-2 R2, stating that it had not assigned a single senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2. SERC staff determined that the issue did not extend back to CIP-003-1 R2 because SERC_URE1 had documented and used its risk-based assessment methodology in 2007 and determined that it had no Critical Assets and therefore no Critical Cyber Assets (CCAs). Pursuant to the applicability section of CIP-003-1, SERC_URE1 was not required to be compliant with CIP-003-1 R2 because it had no CCAs. Upon the effective date of CIP-003-2 R2, however, SERC_URE1 was required by the applicability section of CIP-003-2 to comply with CIP-003-2 R2 even if it found it had no CCAs when using its risk-based assessment methodology. SERC_URE1 still does not have any Critical Assets and therefore has no CCAs. This issue spans versions 2 and 3 of CIP-003.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in the proposed CIP-002-4; and 2. A SERC_URE1's director was responsible for SERC_URE1's compliance with all the NERC Reliability Standards, and SERC_URE1's risk-based assessment methodology was in place and implemented, and reviewed annually by the director with no additions of Critical Assets or CCAs.	SERC staff verified that SERC_URE1 completed the following actions: The SERC_URE1 board of directors passed a board resolution which identified in writing a director as the senior manager with overall responsibility and authority for leading and managing SERC_URE1's implementation of, and adherence to Standards CIP-002 through CIP-009.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2) Nelson Industrial Steam Company (NISCO)	NCRXXXXX	SERC2011007431	CIP-003-2	R2	SERC_URE2 self-reported a possible issue with CIP-003-2 R2, stating that it had not assigned in writing a single senior manager with overall responsibility for leading and managing SERC_URE2's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2. SERC staff determined that the issue did not extend back to CIP-003-1 R2 because SERC_URE2 had documented and used its risk-based assessment methodology in 2008 and determined that it had no Critical Assets and therefore no Critical Cyber Assets (CCAs). Pursuant to the applicability section of CIP-003-1, SERC_URE2 was not required to be compliant with CIP-003-1 R2 because it had no CCAs. Upon the effective date of CIP-003-2 R2, however, SERC_URE2 was required by the applicability section of CIP-003-2 to comply with CIP-003-2 R2 even if it found it had no CCAs when using its risk-based assessment methodology. This issue spans versions 2 and 3 of CIP-003.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4; and 2. During the period of noncompliance, the senior manager was in the same position as now and was in fact responsible for, and had the authority for, leading and managing SERC_URE2's implementation of, and adherence to, Standards CIP-002 through CIP-009, but had not been formally assigned those duties in writing.	SERC staff verified that SERC_URE2 completed the following actions: 1. SERC_URE2 assigned, in writing, a single senior manager with overall responsibility and authority for leading and managing SERC_URE2's implementation of, and adherence to, CIP-002 through CIP-009. 2. SERC_URE2 also developed and implemented a CIP-003 procedure to address the appropriate designation of a senior manager with overall responsibility and authority for leading and managing SERC_URE2's implementation of, and adherence to, CIP-002 through CIP-009.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 3 (SERC_URE3)	NCRXXXXX	SERC2011006618	CIP-002-1	R3	The SERC CIP audit team reported a possible issue with CIP-002-1 R3 because SERC_URE3's Critical Cyber Asset (CCA) list included Cyber Assets that were not essential to the operation of Critical Assets. SERC staff learned the Cyber Assets that SERC_URE3 erroneously included on the CCA list were one router and two firewalls. The router resided outside the Electronic Security Perimeter (ESP) and was mistakenly added to the CCA list. The firewalls are access points to the ESP, and were protected as such, but were inaccurately designated as CCAs by SERC_URE3 personnel.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of bulk power system because the router and two firewalls were not CCAs. The firewalls were access points to the ESP and were being afforded the protective measures pursuant to the CIP Standards. The router never resided within the ESP, was not an access point to the ESP and was not used in the access control and/or monitoring of the ESP.	SERC staff verified that SERC_URE3 completed the following actions: 1. SERC_URE3 removed the three Cyber Assets that were erroneously included on the CCA list. 2. SERC_URE3 added a statement to its CIP cyber security policy that stating that SERC_URE3's list of CCAs will contain explanations for adding or removing assets and will identify the Physical Security Perimeter (PSP) and ESP where the CCA will reside. The CCA list has also been updated to include the additional information regarding the PSP and ESP of the CCA.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 4 (SERC_URE4)	NCRXXXXX	SERC2011008455	CIP-007-3	R4	SERC_URE4 self-reported a possible issue with CIP-007-3 R4 after inadvertently allowing an approved Technical Feasibility Exception (TFE) to expire. SERC_URE4 had submitted a TFE with an open-ended expiration date for two Cyber Assets (switches), on which anti-virus software and malware prevention tools could not be installed. SERC staff rejected the TFE, requesting that SERC_URE4 revise its explanation for the need for a TFE. SERC_URE4 revised the TFE and resubmitted it as a closed-ended TFE with an expiration date. SERC staff approved the revised TFE. SERC staff determined that SERC_URE4 failed to use anti-virus software and malware prevention tools on two Cyber Assets within an Electronic Security Perimeter (ESP) and did not document compensating measures applied to mitigate risk exposure after allowing an approved TFE to expire.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because although the two Cyber Assets involved are not capable of installing anti-virus software or malware prevention tools, they retained the protection of residing within a Physical Security Perimeter and ESP while not covered by an approved TFE.	SERC staff verified that SERC_URE4 completed the following actions: SERC_URE4 submitted a new TFE request with an open-ended expiration date for the two Cyber Assets on which anti-virus software and malware prevention tools could not be installed in order to prevent this issue from occurring again.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1) City of San Marcos (COSM)	NCRXXXXX	TRE2012009901	CIP-003-3	R2.1	During a compliance audit, Texas RE determined that TRE_URE1 did not assign a single senior manager with overall responsibility and authority for leading and managing implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3, as required by CIP-003-3 R2.1. Texas RE determined that the duration period of this issue was from the day the Standard became mandatory and enforceable for TRE_URE1 through the effective date of its updated procedure, assigning a single senior manager.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by several factors. First, during the period of noncompliance, TRE_URE1 did not possess any Critical Cyber Assets (CCAs), which would require adherence with Standards CIP-002-3 through CIP-009-3. Second, TRE_URE1 stated, and Texas RE confirmed, that a senior manager was in place prior to the date the Standard became mandatory and enforceable. However, this change was not documented within the 30 calendar days of the effective day, as required by CIP-003-3 R2.2. Finally, Texas RE determined that TRE_URE1 has minimal potential impact on the BPS because TRE_URE1's peak load is approximately 120 MW.	A document appointing a senior manager was reviewed by Texas RE and Texas RE determined that this document was valid evidence that TRE_URE1 addressed the requirements of CIP-003-3 R2.1. Texas RE received an attestation letter from TRE_URE1, showing that TRE_URE1 has appointed an individual to serve as a single senior manager previously although it was not documented at the time of the appointment. As a result, Texas RE determined that TRE_URE1 has addressed the requirements of CIP-003-3 R2.1. Completion of the mitigation activities was verified by Texas RE during the compliance audit.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2) CIM Channelview Cogeneration, LLC (CVC)	NCRXXXXX	TRE201100460	CIP-003-1	R2.2; R2.3	Texas RE discovered, during a compliance audit, that TRE_URE2's record identifying the responsible senior manager, with overall responsibility and authority for leading and managing the TRE_URE2's implementation of, and adherence to compliance with CIP-002 through CIP-009, was not signed. Texas RE examined all records that required the senior manager's approval and found that they were signed by a different individual. Also, there was no record to evidence that changes to the named senior manager were documented within 30 calendar days of the effective date of the change. Texas RE determined that TRE_URE2 did not address the requirements of CIP-003-1 R2.2 and R2.3 from the date that CIP-003-2 became enforceable and the requirements for identification of the senior manager and delegate became enforceable for entities without Critical Assets, through the date that the senior manager and delegate were identified and documented.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the issue was documentation related only and the risk was mitigated by several factors. First, the senior manager was identified in an acceptable document that was not signed but was backed up by emails that lead up to the signing of the delegation letter authorizing the plant manager to sign on behalf of the senior manager. Before the CIP-003-1 R2 requirement to document and identify the delegated person became enforceable for TRE_URE2, the plant manager was verbally given delegated authority to sign documents on behalf of the senior manager. As a result, the plant manager did in fact sign documents, including TRE_URE2's risk-based assessment methodology and Critical Assets lists. TRE_URE2 produced an attestation related to TRE_URE2's attempt to document the delegation of authority to the plant manager but the result of that documentation effort could not be provided to Texas RE. TRE_URE2 did not have any Critical Assets or Critical Cyber Assets.	During Texas RE's compliance audit, TRE_URE2 produced a new document that that has been determined by Texas RE to sufficiently address the requirements of CIP-003-2 R2.2 and R2.3. The document identified and designated the senior manager and identified and designated approval authority to the plant manager.

Document Accession #: 20120330-5422 Filed Date: 03/30/2012

Document Content(s)