Federal Energy Regulatory Commission
Washington, D.C. 20426
January 20, 2022

FOIA No. FY19-30 (RC12-6)
Fifty First 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 January 11, 2022, 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. RC12-6, along with the names of six (6) 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 RC12-6.

With respect to the remaining identities of UREs contained in RC12-6, before making a determination as to whether this information is appropriate for release under FOIA, a case-by-case assessment of the requested information must consider the

[1] 5 U.S.C. § 552 (2018).

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

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

Based on the application of the various factors discussed above, I conclude that disclosing the identities of the remaining UREs associated with this docket would create a risk of harm or detriment to life, physical safety, or security because the specified UREs could become the target of a potentially bad actor. Therefore, the information is protected from disclosure under FOIA Exemption 7(F). *See* 5 U.S.C. § 552(b)(7)(F) (protecting law enforcement information where release "could reasonably be expected to endanger the life or physical safety of any individual."). Additionally, the information is protected under FOIA Exemption 3. *See* Fixing America's Surface Transportation Act, Pub. L. No. 114-94, § 61003 (2015) (specifically exempting the disclosure of CEII and establishing applicability of FOIA Exemption 3, 5 U.S.C. § 552(b)(3)); *see also* FOIA Exemption 4. Accordingly, the remaining names of the UREs associated with RC12-6 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: 2022.01.19 15:17:10 -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

- InterPower / AhlCon Partners Limited Partnership [GOP] (IPAC)-.pdf page 29

- InterPower / AhlCon Partners Limited Partnership [GO] (IPAC)-.pdf page 29

- EcoGrove Wind, LLC (EcoGrove)-.pdf page 31

- NRG Rockford LLC-.pdf page 31

- NRG Rockford II LLC-.pdf page 32

- ANP Funding I, LLC (ANP)-.pdf page 34-35

December 30, 2011

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

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

Dear Ms. Bose:

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

This FFT resolves 76 possible violations[5] of 19 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 76 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 DECEMBER 2011 FIND FIX AND TRACK REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

Sarah Rogers*
President and Chief Executive officer
Florida Reliability Coordinating Council, Inc.
1408 N. Westshore Blvd., Suite 1002
Tampa, Florida 33607-4512
(813) 289-5644
(813) 289-5646 – facsimile
srogers@frcc.com

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

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

FOR MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
(651) 855-1731
dp.skaar@midwestreliability.org

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

FOR RFC:

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

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

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

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

FOR SERC:

R. 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

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

Kenneth B. Keels, Jr.*
Director of Compliance
Andrea Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive
Charlotte, NC 28217
(704) 940-8214
(704) 357-7914 – facsimile
kkeels@serc1.org
akoch@serc1.org

FOR SPP RE:

Stacy Dochoda*
General Manager
Southwest Power Pool Regional Entity
16101 La Grande, 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 La Grande, 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 La Grande, 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

FOR NCEA:

Sean Bodkin
Compliance Enforcement Coordinator
North American Electric Reliability Corporation
1325 G Street NW, Suite 600
Washington, DC 20005
(202) 400-3000
sean.bodkin@nerc.net

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
December 30, 2011

Take notice that on December 30, 2011, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding forty (40) Registered Entities in seven (7) Regional Entity footprints and NERC as the Compliance Enforcement Authority.

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_URE1)	NCRXXXXX	FRCC2011008541	CIP-007-1	R4	The entity self-reported an issue with CIP-007-1 R4. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity installed two network switches and ten vibration monitoring systems for which it was technically infeasible to install anti-malware. The entity installed comparable compensating and mitigating measures by implementing procedural controls to require review for authenticity prior to installation of any application or firmware. The TFE submittals were 65 and 306 days late.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measure to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network separation and only allowed the required communication through the network. The network is protected by firewall in a designated Electronic Security Perimeter. The entity also implemented manual controls to perform review of all new installation of patches and firmware to ensure source and integrity validation. This process also includes vendor certification and hash value integrity check. Further, the entity is utilizing intrusion detection systems to perform network packet/traffic scan and alerting for malware signatures.	The entity submitted two Technical Feasibility Exceptions (TFEs) that were accepted by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008542	CIP-007-1	R5; R5.3; R5.3.2	The entity self-reported an issue with CIP-007-1 R5. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity installed one terminal server, four printers, 32 network switches, 26 micro controllers, seven routers, 168 servers and desktops, and ten vibration monitoring devices, where it was technically infeasible to enforce compliance with the password requirements of R5.3 and password complexity requirements of R5.3.2. The entity implemented compensating measures at the time of implementation but submitted late TFEs 37 to 306 days after the safe harbor date.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measure to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network separation and only allowed the required communication through the network. The network is protected by the firewall in a designated Electronic Security Perimeter. The entity has also implemented manual controls designed to increase user awareness for password compliance requirements, perform manual review of all password for complexity, created annual schedule of required password change. Further, where the passwords cannot meet the CIP requirements for complexity and character length, the entity manual controls require the user to ensure that passwords are created to apply the maximum technically feasible complexity and the length.	The entity submitted seven Technical Feasibility Exceptions (TFEs) that were accepted by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008543	CIP-007-1	R2; R2.3	The entity self-reported an issue with CIP-007-1 R2. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity installed eight vibration monitors, eight micro controllers and two terminals where it was technically infeasible to stop/disable ports and services that were enabled on the devices. The entity implemented compensating measures at the time of implementation but submitted late TFEs 220 days after the safe harbor date.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measure to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network/VLAN separation and only allowed the required communication through the network. The network is protected by the firewall in a designated Electronic Security Perimeter. Further, the entity utilizes intrusion detection systems to perform network packet/traffic scan and alerting for malware signatures.	The entity submitted one Technical Feasibility Exception (TFE) that was accepted by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008544	CIP-007-1	R6; R6.3	The entity self-reported an issue with CIP-007-1 R6. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity installed 66 switches, two routers, 56 micro controllers, 22 vibration sensors and 13 servers where it was not technically possible to meet CIP-007-3 R6 and R6.2. The entity implemented compensating measures at the time of implementation but submitted late TFE requests were submitted 408 days after the safe harbor date.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measures to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network/VLAN separation and only allowed the required communication through the network. The network is protected by the firewall in a designated Electronic Security Perimeter. Further, the entity utilizes intrusion detection systems to perform network packet/traffic scan and alerting for malware signatures.	The entity submitted 12 Technical Feasibility Exceptions that were accepted by FRCC.

Attachment A-1

December 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

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	FRCC201100418	VAR-002-1.1a	R3	The entity self-certified non-compliance with VAR-002-1.1a R3. The entity's energy control center and plant logs revealed that on 5/7/2010, the entity's generating unit operator did not communicate to the Transmission Operator (TOP) the Automatic Voltage Regulator's (AVR) "automatic" to "manual" mode status change within 30 minutes nor did it communicate how long the AVR would remain in manual. Although there is no evidence that the TOP was ever notified by the entity, the TOP did have status display of the entity's AVR on its Energy Management System (EMS) screens. There is no issue with R1, as the entity under normal conditions did operate each generator connected to the interconnected transmission system in the automatic voltage control mode; however, in this instance the AVR control logic failed and caused a malfunction to manual mode causing an inadvertent status change. Therefore, FRCC did not apply R1 to this issue as R3 was considered the applicable requirement due to the inadvertent status change.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system since the Generator Operators were still controlling voltage manually. In addition, the TOP did have indication through the EMS of AVR status. Furthermore, this issue was limited to a single instance. Lastly, the unit was only in "manual" mode for 12 minutes before being returned to "automatic."	The entity conducted a diagnostic/ evaluation process focused on identifying improvement opportunities, in order to mitigate opportunities for additional reportable incidents. The extensive process required the entity to thoroughly review each of the VAR-002 requirements and identify improvement opportunities to achieve compliance. As a result of this process, it was determined that a user-friendly, web-based reporting tool should be developed by creating a new module in the entity's program for the plant operators and energy control center TOPs to communicate and acknowledge the plant Reactive Power status (mode) and capability changes. The entity's operations group issued an order to all of its generating facilities that reiterated the requirements in VAR-002 as well as the logging, documentation, and data retention period requirements. This new module tool will go through funding approval, design, and development, then the reporting tool Beta testing will commence. Operator training was completed after completion of the Beta testing and full implementation of this new reporting tool began.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100431	PRC-005-1	R2; R2.1; R2.2	The entity self-reported an issue with PRC-005-1 R2. The entity's contract technician completed the replacement of a 230 kV primary line relay. After the work was completed, an employee of the entity interpreted the test results documentation received as covering the complete primary and backup relay groups and closed the work order for both primary and backup relay groups. This created an incorrect due date on all the relays (except for the one primary relay replaced as described above) of both primary and backup relay groups of four years from the replacement date. The remaining relays (one primary and one backup) exceeded their allowable maintenance and testing interval. To resolve the issue with the relays, the backup relay group was maintained 3 months past the correct due date and primary relay groups were maintained approximately one year and three months later.	This issue posed a minimal and not serious or substantial risk to the bulk power system since the entity's primary and backup relay group was tested correctly (within the entity's PRC-005 program requirements) and found to be operational. In addition, no misoperations were reported for this line during the time period of the missed testing and testing was only out of interval for 98 days.	As part of the entity's continuing effort to improve NERC compliance, new processes and procedures have been implemented. These process improvements include a review of documentation to close work orders. This procedure was created as a result of the PRC-005 mitigation plan and describes the roles and responsibilities of personnel involved in the planning, scheduling and closing of work orders. In addition, the entity has implemented an equipment change request process that is designed to be a barrier to the corruption of the equipment database. The equipment change request process was rolled out as part of the mitigation plan, and serves as a tool to ensure the entity's equipment database accurately represents the Protection System assets that are in the field. equipment change requests provide updates to the database as changes occur via the entity's protection engineering, construction and maintenance organization activities. To bring these relays back into compliance, the backup and primary relay groups were maintained.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC2011008531	CIP-007-1	R5; R5.3	The entity self-reported an issue with CIP-007-1 R5. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity's TFE for the ten firewalls was submitted 397 days after installation of the devices. These firewalls do not have the capability to enforce password complexity as required by CIP-007 R5.3. While the devices do support acceptable passwords there is no technical mechanism to enforce it. This TFE includes ten firewalls and was late by 397 days.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system because even though the TFE request was submitted late, the following compensating and mitigating measures were implemented at the time of device installation. The firewalls are on a private network as the separation point between the general business traffic and the control center network. Additionally, all network traffic to these devices is monitored by the entity's intrusion detection system. The entity also implemented procedural controls to ensure that all passwords comply to highest technically feasible complexity.	The entity has submitted one Technical Feasibility Exception that was accepted and approved by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011008528	CIP-007-1	R2; R2.3	The entity self-reported an issue with CIP-007-1 R2. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity has two micro controllers where it is technically infeasible to disable unused ports and services as required by the Standard. The entity implemented comparable security measures but failed to submit the TFE before the safe harbor date. The TFE was late by 188 days.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measure to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network/VLAN separation and only allowed the required communication through the network. The network is protected by the firewall in a designated ESP. Further, the Responsible Entity is utilizing intrusion detection systems to perform network packet/traffic scan and alerting for malware signatures.	The entity has submitted one Technical Feasibility Exception that was accepted and approved by FRCC.

Attachment A-1

December 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

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 3 (FRCC_URE3)	NCRXXXXX	FRCC2011008529	CIP-007-1	R5; R5.3.2	The entity self-reported an issue with CIP-007-1 R5. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity has 20 operating systems where enforcing a combination of alpha, numeric and "special" characters for passwords as required by CIP-007 R5.3.2 is not technically feasible. The entity implemented comparable security measures but failed to submit the TFE before the safe harbor date for 20 of these systems. The TFE was late by 188 days.	FRCC determined this issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system, because this issue was due to late submission of the TFE and all mitigation and compensating measure to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented the following compensating measures. The entity implemented technical controls such as network separation and only allowed the required communication through the network. The network is protected by the firewall in a designated Electronic Security Perimeter. The entity also implemented manual controls designed to increase user awareness for password compliance requirements, perform manual review of all password for complexity, created annual schedule of required password change. Further, where the passwords cannot meet the CIP requirements for complexity and character length, the entity manual controls require the user to ensure that passwords are created to apply the maximum technically feasible complexity and the length.	The entity has submitted one Technical Feasibility Exception that was accepted and approved by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007860	PRC-023-1	R1	During a compliance audit the entity was found to have an issue with PRC-023-1 R1. The entity's documents, in addition to subject matter expert interviews were insufficient to demonstrate that the entity set one of its 59 transmission line relays so that it did not operate at or below 150% of the highest seasonal Facility Rating of the circuit, for the available defined loading duration nearest four hours (expressed in amperes). The maximum primary ohm value the relay zone should be set at was 25.083 ohms. The entity's relay was set at 25.536 ohms (148.2%) which is below the 150% requirement and greater than the maximum primarily setting allowed.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system since the relay was only 1.8% off from the necessary value, it was an overreaching relay that would have tripped after the primary relay set detected a fault and tripped and it was only one of 59 relays out of calibration and only out of calibration for 98 days.	The entity re-computed, coordinated and reset the protective relay to achieve 150% loadability as required by the Standard.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007861	PRC-001-1	R3; R3.2	During a compliance audit the entity was found to have an issue with PRC-001-1 R3. The entity's documents were insufficient evidence to demonstrate that the entity, coordinated all new protective systems and all protective systems changes with its neighboring Transmission Operators and Balancing Authorities.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system since the entity had performed initial internal screening of changes to major transmission lines but determined the changes only affected the entity and not interconnections or neighboring Transmission Operators or Balancing Authorities.	The entity performed the following mitigation activities: 1. Reported and coordinated all changes of protection systems with all neighboring Transmission Operators (TOPs), Generator Operators (GOPs) and Balancing Authorities (BAs); 2. Instructed system protection group management to coordinate all new and modified protection systems with system operations, which will coordinate with neighboring TOPs, GOPs and BAs, until a new permanent procedure is in place; and 3. Developed and implemented a new procedure for the coordination of all new and modified protection systems with neighboring TOPs, GOPs and BAs.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007862	PRC-001-1	R4	During a compliance audit the entity was found to have an issue with PRC-001-1 R4. The entity's documents were insufficient evidence to demonstrate that the entity coordinated protection systems on major transmission lines with neighboring Generator Operators, Transmission Operators and Balancing Authorities.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system since the entity had performed initial internal screening of changes to major transmission lines but determined the changes only affected the entity and not interconnections or neighboring Transmission Operators or Balancing Authorities.	The entity performed the following mitigation activities: 1. Reported and coordinated all changes of protection systems with all neighboring Transmission Operators (TOPs), Generator Operators (GOPs) and Balancing Authorities (BAs); 2. Instructed system protection group management to coordinate all new and modified protection systems with system operations, which will coordinate with neighboring TOPs, GOPs and BAs, until a new permanent procedure is in place; and 3. Developed and implemented a new procedure for the coordination of all new and modified protection systems with neighboring TOPs, GOPs and BAs.

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 4 (FRCC_URE4)	NCRXXXXX	FRCC2011008526	CIP-006-1	R1; R1.1	The entity self-reported an issue with CIP-006-1 R1. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity submitted three late TFEs for three of its Physical Security Perimeters (PSPs) that could not implement a complete six-walled perimeter due to excessive cost implications. While the entity submitted the TFE later than the safe harbor date, it did implement comparable security measures. The TFE was late by 113 days.	FRCC determined this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system because this issue was due to late submission of the TFE. In addition, all mitigating and compensating measures to provide comparable security were in place at the time of implementation of the PSPs. The following compensating and mitigating measures were implemented prior to TFE acceptance/approval by FRCC. The PSPs are within a facility that is guarded 24 hours a day, seven days a week, and only authorized entity personnel have access to the facility. All PSPs have access controls including locked doors and card readers with alarms. In order to compensate the lack of complete six-wall boundary due to use of raised floors and false ceilings in some areas, the entity has implemented mesh of bars that limit access. Further, all the Cyber Assets are inside locked cabinets and only authorized personnel have access to these locked cabinets.	The entity submitted one late Technical Feasibility Exception that was approved by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 4 (FRCC_URE4)	NCRXXXXX	FRCC2011008527	CIP-007-1	R6; R6.3	The entity self-reported an issue with CIP-007-1 R6. This issue is a result of the entity's failure to timely submit Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The entity has a single GPS clock source that is not able to comply with CIP-007-1 R6 due to technical limitations. The entity implemented comparable security measures but submitted the TFE later than the safe harbor date. The TFE was late by 113 days.	FRCC determined this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system because this issue was due to late submission of the TFE. In addition, all mitigating and compensating measures to provide comparable security were in place at the time of implementation of these Cyber Assets. The following compensating and mitigating measures were completed prior to the TFE approval. The entity implemented technical controls such as network/VLAN separation and only allowed the required communication through the network. The network is protected by the firewall in a designated Electronic Security Perimeter. Further, the entity utilizes intrusion detection systems to perform network packet/traffic scan and alerting for malware signatures.	The entity submitted one late Technical Feasibility Exceptions that was approved by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 5 (FRCC_URE5)	NCRXXXXX	FRCC2011008530	CIP-007-1	R4	The entity self-reported an issue with CIP-007-1 R4. This issue is on account of entity's failure to timely submit a Technical Feasibility Exception (TFE) request in accordance with NERC procedures. The entity installed three physical access control system microcontrollers for which no anti-malware is available. The TFE was submitted late by 274 days.	FRCC determined this issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system because this issue was due to late submission of the TFE. In addition, all mitigating and compensating measures to provide comparable security were in place at the time of implementation of these Cyber Assets. The entity implemented technical controls such as network separation and only allowed the required communication through the network. The network is protected by firewall in a designated Electronic Security Perimeter. The entity also implemented manual controls to perform review of all new installation of patches and firmware to ensure source and integrity validation.	The entity submitted one late Technical Feasibility Exceptions that was approved by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 6 (FRCC_URE6)	NCRXXXXX	FRCC201000412	INT-006-3	R1	The entity self-reported an issue with INT-006-3 R1. The entity failed to respond within ten minutes to each Request for Interchange (RFI) and any modifications to RFI, that were submitted between 15 minutes and one hour of the ramp start time of the Arranged Interchange. The entity found 24 instances where electronic tags were allowed to expire before approvals (or a response) were made to transition an Arranged Interchange to a Confirmed Interchange. 21 of the 24 events were due to the entity failing to respond to an on-time RFI or adjustment to an RFI before it expired. One was due to the entity failing to respond to an on-time extension to an RFI and two were a termination or cancellation of an RFI.	This issue posed a minimal and not serious or substantial risk to the reliability of the bulk power system since none of the RFI, that expired before the entity could respond, were due to an emergency or a reliability adjustment. Therefore they only affected commercial transactions, not reliability transactions. Also, there were only 24 expired tags during the roughly one year period ranging from 18 MW to 220 MW and all 24 tags were under normal conditions. In addition, there were no reliability impacts from these events.	The entity performed the following mitigation activities: 1) Reminded all energy system operators, via email, to perform reliability assessments, per INT-006-3 R1, and act on all tags before they expire; 2) Posted an announcement in the energy control center site that reiterates the requirement regarding expiration of tags. The announcements of the site are visible at all times to all on-duty energy system operators in the control center; 3) Installed an additional monitor screen for reviewing tags to assist in responding to interchange requests on time; 4) Trained energy system operators regarding the timing requirements on all tags to prevent the expiration of tags. Provided training to the energy system operators of a vendor's tag request approval monitor program and communicated how this program prioritizes tags by expiration time; 5) Initiated a periodic review of tags to check for compliance through the completion of this mitigation plan; 6) Communicated the issue to the vendor regarding electronic tag and other programs freezing up. Notified and requested from the vendor a greater understanding of the problem and acquired recommendations from the vendor to mitigate the problem; 7) Discussed with other local Florida utilities as to how they process their tags and whether any other mitigation steps should be taken; 8) Completed investigation of the option of having either the other program or electronic tag system automatically approve or deny tags before they expire and whether this option could help achieve on-time response without undesirable consequences; and 9) The investigation revealed the best course would be to implement and test an automatic deny feature. If the operator cannot complete the reliability assessment of a tag within the appropriate timeframe, it will be automatically denied before it expires. Automatic approval was not implemented because a complete reliability assessment could not be automatically performed with the program.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100406	CIP-005-1	R3; R3.2	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-005-1 R3. The TFE request was submitted approximately two months beyond the required TFE submission window. The entity requested the TFE because the Cyber Assets used to control and monitor physical access to the entity's Physical Security Perimeter do not support security monitoring processes that alert for attempts at or actual unauthorized accesses.	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 implemented the following compensating measures: (1) located the Cyber Assets within a Physical Security Perimeter; (2) manually reviewed access logs; and (3) isolated Cyber Assets from the corporate network, Supervisory Control and Data Acquisition (SCADA) system and the internet. The only logical access to the system is in the data center and is protected by strong passwords. Additionally, these compensating measures were in place prior to the date on which the TFE request was originally due to MRO.	The entity performed a new analysis of its risk-based assessment methodology and subsequently declared no Critical Assets or Critical Cyber Assets. The devices were covered by appropriate compensating security measures while in service and declared as Critical Cyber Assets. MRO terminated the TFE.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100407	CIP-007-1	R2; R2.3	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R2. The TFE request was submitted approximately two months beyond the required TFE submission window. The entity requested the TFE because several Cyber Assets do not support the disabling of unused ports and services. The system is not vendor-supported due to system age, and attempts to disable ports and services will have adverse operational effects.	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 following compensating measures were in place: (1) the Cyber Assets are located in a Physical Security Perimeter; and (2) the Cyber Assets are isolated from the corporate network, SCADA system and the internet. The only logical access to the system is in the data center and is protected by strong passwords. Additionally, these compensating measures were in place prior to the date on which the TFE request was originally due to MRO.	The entity performed a new analysis of its risk-based assessment methodology and subsequently declared no Critical Assets or Critical Cyber Assets (CCAs). The devices were covered by appropriate compensating security measures while in service and declared as CCAs. MRO terminated the TFE.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100408	CIP-007-1	R4	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R4. The TFE request was submitted approximately two months beyond the required TFE submission window. The entity requested the TFE because several physical access control systems did not support the installation of anti-virus or malware prevention software. Additionally, the system is not vendor supported due to system age, and an attempt to install anti-virus software would have an adverse operational affect.	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 following compensating measures were in place: (1) the Cyber Assets covered by this TFE are located within the Physical Security Perimeter; (2) the Cyber Assets are isolated from the corporate network, Supervisory Control and Data Acquisition (SCADA) system and the internet; the only logical access to the system is in the data center and is protected by strong passwords; and (3) all devices used for maintenance activities are scanned for viruses and malware prior to connection to these covered Cyber Assets.	The entity performed a new analysis of its risk-based assessment methodology and subsequently declared no Critical Assets or Critical Cyber Assets (CCAs). The devices were covered by appropriate compensating security measures while in service and declared as CCAs. MRO terminated the TFE.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100409	CIP-007-1	R6	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R6. The TFE request was submitted approximately two months beyond the required TFE submission window. The entity requested the TFE because several of the entity's devices did not support automated tools to monitor system events related to cyber security. Attempts to install automated monitoring would have an adverse operation effect on system configurations.	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 has the following compensating measures in place: (1) the Cyber Assets covered are located within a Physical Security Perimeter; (2) the Cyber Assets are isolated from the corporate network, Supervisory Control and Data Acquisition (SCADA) system and the internet; the only logical access is through the data center which is protected by strong passwords; and (3) logs and system events are reviewed annually.	The entity performed a new analysis of its risk-based assessment methodology and subsequently declared no Critical Assets or Critical Cyber Assets (CCAs). The devices were covered by appropriate compensating security measures while in service and declared as CCAs. MRO terminated the TFE.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100410	CIP-007-1	R2; R2.3	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R2. The TFE request was submitted approximately one year beyond the required TFE submission window. The entity requested the TFE because several substation meters and card reader access controls have unused ports and services which cannot be disabled.	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 TFE was approved by MRO and the entity has the following compensating measures: (1) The substation meter is connected to the substation Electronic Security Perimeter (ESP) switch that is in a locked cabinet. The switch enforces that all connecting devices are authorized by media access control address, and restricts connections between pre-defined source and destination switch ports only; (2) remote access into the substation WAN is only allowed from designated support stations in Physical Security Perimeters (PSP), and the vulnerable IP ports are restricted by policy; (3) the ESP firewall logs remote access events and policy violations to a central log server; (4) the substation LAN is monitored by an intrusion detection system that detects protocol anomalies; (5) access logs are manually reviewed typically every business day, but never more than 30 days later; (6) all controller devices are isolated as the sole network device in an ESP behind a firewall. The firewall policy allows remote access only by the card access server on the authorized port. The firewall restricts the controller device from initiating any outbound connection, only communicating with establish incoming communications; (7) for controller devices on the central card access LAN ESP, no external hosts are allowed to communicate with these devices via configuration; and (8) the controllers and firewalls are always inside of a PSP.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201100411	CIP-007-1	R5; R5.3	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R5. The TFE request was submitted one year beyond the required TFE submission window. The entity requested the TFE because a legacy Inter-Control Center Protocol (ICCP) application server has user accounts and passwords embedded in the software that cannot be changed because the vendor no longer supports the system.	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 TFE was approved by MRO and the entity has the following compensating measures: (1) pre-defined external connections allowed with peer hosts communicating on the port have been removed. The only remaining data links are to other internal systems in the same Physical Security Perimeter as these servers; (2) a new firewall and perimeter network has been implemented, and direct incoming access to this host is no longer allowed; and (3) external support access from authorized hosts must use indirect access, after establishing a session to an allowed host.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3)	NCRXXXXX	MRO201100415	CIP-007-1	R4	The entity failed to submit timely Technical Feasibility Exception (TFE) requests in accordance with NERC procedures for CIP-007-1 R4. The TFE requests were submitted approximately four months and fourteen months beyond the required TFE submission window. The entity requested the TFE because Cyber Assets detailed in the TFE are network firewalls that do not support the use or running of anti-virus or malware prevention tools. Per the manufacturer attestation and documentation, the devices are not susceptible to malware or viruses. The entity has provided a document attesting to the fact that the systems do not support the use of anti-virus or other malware prevention tools. Additionally, the TFE covers network routers, switches and telecommunications devices that that do not support the use or running of anti-virus or malware prevention tools.	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 entity has the following compensating measures: (1) access is protected by Electronic Security Perimeter (ESP) and login access control; (2) the Cyber Assets reside within a second tier Physical Security Perimeter controlled by cyber locks to intentionally reduce and control log access to the device; (3) logical and electronic access is controlled and restricted to personnel with the “need to know” job criteria; (4) anti-virus and malware prevention tools are implemented on all other Cyber Assets within the ESP(s) where capable; and (5) hardware, firmware and software for the Cyber Assets are frozen; the covered assets are to conform to their corresponding frozen versions in order to be in the system.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3)	NCRXXXXX	MRO201100417	CIP-007-1	R5; R5.3	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R5. The TFE was submitted approximately 10 months beyond the required TFE submission window. The entity requested the TFE because the devices detailed in this TFE are network servers running databases that are tightly coupled to the entity's transmission management system (TMS) application. A small number of administrative accounts are utilized by the TMS application for database access and currently cannot be changed without impact on the functioning of that application.	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 entity has the following compensating measures: (1) the covered Cyber Asset is protected by an Electronic Security Perimeter; (2) the covered asset is a purpose built device with a hardened operating system; and (3) access to the covered asset is via user identification and password login access control.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100418	CIP-007-1	R2; R2.3	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R2. The TFE request for the entity was submitted approximately three months late. The entity requested the TFE because the devices detailed in this TFE are two application servers where the entity has not been able to disable unused ports and services declaring that it is currently infeasible and would introduce operational risk to the Energy Management System (EMS). To the extent possible, the entity has worked with EMS vendor to define and document all ports and services for these covered Cyber Assets. To date, a complete list has not been attainable and this is the basis for the TFE.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO considered that the vendor has performed system hardening on all operating systems that are part of the Energy Management System and network during the last EMS upgrade completed in April 2008, enabling only ports and services that at that time were known to be necessary for normal and emergency operations. Host-based intrusion detection systems (HIDS) agents are running on all EMS systems providing host-based firewall and anti-virus/malware protection services. The entity has configured host-to-host connection restrictions within the Electronic Security Perimeter (ESP) enforced by the HIDS. Access to EMS host systems within the ESP is provided by multiple levels of host-based and network based authentication. Remote access into the ESP is managed through secure virtual private network (VPN) appliances using two-factor authentication.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100419	CIP-005-1	R2; R2.6	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-005-1 R2. The TFE request for the entity was submitted approximately eight months late. The entity requested the TFE because the devices detailed in this TFE are LAN controllers for the physical access control system that do not support the use of or installation of appropriate use banners.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO considered that the LAN controllers reside within defined Physical Security Perimeters (PSPs); interactive management access to the LAN controllers is restricted to only connections originating at the access control system server; and there is real-time logging of all connections to the LAN controllers.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100420	CIP-007-1	R4	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R4. The TFE request for the entity was submitted approximately eight months late. The entity requested the TFE because the devices detailed in this TFE are LAN controllers for the access control system that do not support the use of or installation of anti-virus or malware prevention tools. The entity provided vendor attestation that these devices cannot deploy anti-virus and malware prevention tools.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO considered that the LAN controllers reside within defined Physical Security Perimeters (PSPs); interactive management access to the LAN controllers is restricted to only connections originating at the access control system server; and there is real-time logging of all connections to the LAN controllers.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5)	NCRXXXXX	MRO201100421	CIP-007-1	R3	The entity failed to submit timely Technical Feasibility Exception (TFE) requests in accordance with NERC procedures for CIP-007-1 R3. The TFE requests for the entity were submitted between two months and seven months late. The entity requested the TFE because the devices detailed in these TFE requests are a security information management system, a server running proprietary load management software, two modems, a remote access server providing dial-in access and data storage appliances that cannot support the installation of security patches or updates.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO considered that the security information management system resides within a defined Electronic Security Perimeter (ESP) with limited access to the system, resides within a defined Physical Security Perimeters (PSPs), has a hardened operating system with no administrative access to the system or software for the users, and devices communicating with the security information management system are regularly patched per the entity's security patch management program. MRO considered that the data storage appliances reside within a defined ESP and PSP. MRO considered that the modems connect to a Cyber Asset that has security patches and updates deployed per the entity's security patch management program and communication to and from the devices uses a non-routable protocol. MRO considered that the remote access server connects to a Cyber Asset that has security patches and updates deployed per the security patch management program; external communication to/from the device uses a non-routable protocol; access and use of the modem is controlled through the use of a password authentication and remote controlled relay switch. The switch allows a system operator to remotely enable the modem for a requested period of time for an authorized user. Also, an alert is sent to the Energy Management System (EMS) analyst whenever the modem is connected. Additionally, all communication with devices within the ESP is monitored by a security information and event management system and controlled via firewall access point policy.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests. The entity has installed a new server which allows application of security patches and updates. MRO approved termination of the TFE related to the first identified server. The entity removed the remote access dial-in server and a modem from the EMS network. MRO approved termination of the TFEs related to the remote access server and one modem. The entity removed the data storage appliances from the EMS network. MRO approved termination of the TFE related to the data storage appliances.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5)	NCRXXXXX	MRO201100422	CIP-007-1	R4	The entity failed to submit timely Technical Feasibility Exception (TFE) requests in accordance with NERC procedures for CIP-007-1 R4. The TFE requests for the entity were submitted between four months and nine months late. The entity requested the TFEs because the devices detailed in these TFEs are a security information management system, extreme network switches, and a virtual private network (VPN) appliance that do not support the use or running of anti-virus or malware prevention tools.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO considered that the security information and event management (SIEM) system resides within a defined Electronic Security Perimeter (ESP) with limited access to the system, resides within a defined Physical Security Perimeter (PSP), has a hardened operating system with no administrative access to the system or software for the users, and devices communicating with the security management information system are regularly patched per the security patch management program. MRO considered that the extreme network switches reside within a defined ESP and PSP, and all Cyber Assets connected to the network switch that are capable of running anti-virus and malware prevention tools have those services installed and running. MRO considered that remote access sessions initiated by the VPN appliance are directed to firewall access points for network and host access control; only identified users are configured in and allowed access via the VPN appliance; and all ESP data traffic and the VPN appliance are monitored by SIEM.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 6 (MRO_URE6)	NCRXXXXX	MRO201100423	CIP-007-1	R4	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R4. The TFE request for the entity was submitted approximately three months late. The entity requested the TFE because the devices detailed in this TFE are network switches, encryption devices and remote terminal units (RTUs) that do not run anti-virus software or services. The entity has provided vendor documentation and attestation that the devices cannot use anti-virus software or other malware prevention tools.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failure by the entity to comply with the administrative process for the submission of a formal TFE request. The devices reside within a defined Electronic Security Perimeter (ESP) and are protected by firewalls with appropriate policies blocking access to these devices. Remaining Critical Cyber Assets and Cyber Assets within the ESP that are capable of using and running anti-virus software and malware prevention tools have those services implemented.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 6 (MRO_URE6)	NCRXXXXX	MRO201100424	CIP-007-1	R6	The entity failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures for CIP-007-1 R6. The TFE request for the entity was submitted approximately three months late. The entity requested the TFE because it has provided vendor documentation and attestation that the remote terminal units (RTU) devices cannot implement automated tools or organizational process controls to monitor system events that are related to cyber security.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failure by the entity to comply with the administrative process for the submission of a formal TFE request. The devices reside within a defined Electronic Security Perimeter (ESP) and are protected by firewalls with appropriate policies blocking access to these devices. Remaining Critical Cyber Assets and Cyber Assets within the ESP that are capable of using and running anti-virus software and malware prevention tools have those services implemented.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 7 (MRO_URE7)	NCRXXXXX	MRO201100291	CIP-007-1	R4	The entity self-reported an issue with CIP-007-1 R4 because it failed to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures. The TFE request for the entity was submitted approximately ten months late. The entity requested the TFE because it utilizes anti-virus software on all non-Energy Management System (EMS) equipment located within the defined Electronic Security Perimeter, however anti-virus software was not installed on any communication front end device because the EMS vendor did not have an anti-virus product certified for use with the software release currently running on the system. The critical performance of communication for Supervisory Control and Data Acquisition (SCADA) would not afford the necessary resource to run virus scanning while performing the real-time SCADA function.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failure by the entity to comply with the administrative process for the submission of a formal TFE request. During the duration of the TFE, the entity did not allow direct internet connections or email accounts on the Energy Management System (EMS). Additionally for all EMS equipment, the autorun and autoplay features were disabled.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests. This TFE has been terminated because the entity completed the installation of anti-virus software on the covered Cyber Assets.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 8 (MRO_URE8)	NCRXXXXX	MRO201100426	CIP-007-1	R4	The entity failed to submit timely Technical Feasibility Exception (TFE) requests in accordance with NERC procedures for CIP-007-1 R4. The TFE requests for the entity were submitted approximately four months late. The entity requested the TFE because the devices detailed in these TFE requests are network switches, fiber channel switches, data storage components, network security appliances and firewalls, terminal servers that provide serial-to-ethernet conversion, protocol converters, splitter panels used for sharing modem connections between front-end processors (FEPs), and a printer that do not run anti-virus software or services. The entity has provided vendor documentation that the devices do not use or run anti-virus software or other malware prevention tools.	MRO determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because the issue resulted from failures by the entity to comply with the administrative process for the submission of a formal TFE request. MRO determined that the hardened design of the devices, redundancy of critical components, use of intrusion detection software and a monitoring, analysis and response system to detect malicious activity and administrator notifications of potential security events minimize risk, to the extent possible, of adverse impact to the covered Cyber Assets.	The entity mitigated the issue by submitting all acceptable TFE requests and has continuously performed all of the compensating measures as discussed in the TFE requests.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 9 (MRO_URE9)	NCRXXXXX	MRO201000169	PRC-005-1	R2; R2.1; R2.2	The entity self-reported an issue with PRC-005-1 R2 because it failed to maintain records for some of its station batteries. Upon receiving the Self-Report, MRO requested a full inventory of the entity's maintenance and testing records for its transmission Protection System devices. The entity reported that it has over 300 Protection System devices subject to PRC-005-1 R2. Of these devices, the entity failed to provide maintenance and testing records for approximately 8.6% of the devices, including station batteries, DC control circuits, voltage and current sensing devices and associated communication systems. Therefore, MRO determined that the entity failed to provide evidence of maintenance and testing records for its Protection System devices as required by PRC-005-1 R2.1 and R2.2.	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 was able to provide evidence of maintenance and testing records for 91% of its Protection System devices. Additionally, some of the devices were monitored periodically or continuously via the entity's Supervisory Control and Data Acquisition (SCADA) system, and upon testing the devices with missing records, the entity did not identify any issues related to performance.	The entity performed a full review of its maintenance and testing records for its Protection System components and completed maintenance and testing on its devices missing records. The entity completed mitigation activities, as verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 10 (MRO_URE10)	NCRXXXXX	MRO201100246	EOP-004-1	R3	The entity self-reported an issue with EOP-004-1 R3 because it failed to provide MRO and NERC with a preliminary written report within 24 hours of a reportable incident. The entity began drafting and adopted a procedure in order to report incidents as required by the Standard a few months later. While drafting the procedure, the entity discovered that it had failed to report an incident as required by the Standard and therefore, self-reported the issue.	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 soon after the event, the entity analyzed the service disruption as intended by the Standard and subsequently carried out repairs to address the root cause of the disruption as identified by the analysis. The entity also provided a preliminary written report to MRO and NERC.	The entity provided a preliminary written report to MRO and NERC. Additionally, the entity developed and documented a training procedure for operators to report incidents as required by the Standard. The entity also developed internal controls to ensure that all events are reported to the proper authority.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC2011001051	CIP-004-3	R2	The entity self-reported a possible issue with CIP-004-3 R2 to Reliability*First.* The entity discovered that it granted an employee who had not completed the entity's CIP training unescorted physical access to one Physical Security Perimeter (PSP) containing Critical Cyber Assets (CCAs). The entity revoked the employee's access after it discovered the issue through its daily reconciliation of employee access rights. Reliability*First* determined that the entity had an issue with the Standard as it failed to ensure that the employee received CIP training prior to granting that employee unescorted physical access to the PSP containing CCAs.	The risk to the reliability of the bulk power system was mitigated by the following factors. The employee to whom the entity granted unescorted physical access had successfully completed similar initial and annual CIP training required by the entity's affiliates. Also, the employee at issue had been subject to a personnel risk assessment prior to the issue. In light of the nature of the issue, offset by the aforementioned mitigating factor, Reliability*First* determined that this issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First*. The entity revised its procedure for granting physical access to require a supervisor to approve and implement all requests for access to PSPs. The entity also conducted training on the revised procedure for all relevant employees. In this mitigation plan, the entity represented that it completed the mitigating actions.

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	RFC201000997	FAC-001-0	R2; R2.1.3	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered a possible issue associated with FAC-001-0 R2.1.3. Reliability*First* determined that the facility connection requirements documentation the entity provided did not address MW and MVAR capacity or demand at the point of connection pursuant to FAC-001-0 R2.1.3. Although the entity stated that it relies on interconnection requirements put forth by its Transmission Operator, it failed to provide Reliability*First* with documentation reflecting this reliance. Additionally, neither the entity's internal documents nor the PJM manuals the entity provided to Reliability*First* address MW and MVAR capacity or demand at point of connection. Reliability*First* determined that the entity, as a Transmission Owner, failed to provide evidence that it addressed MW and MVAR in its facility connection requirements pursuant to FAC-001-0 R2.1.3.	In the light of the nature of the issue, offset by the following mitigating factors, Reliability*First* determined that this issue posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). The entity has had a documented transmission planning procedure in place. During the compliance audit, Reliability*First* determined the entity satisfied all of FAC-001-0 R2's sub-requirements except R2.1.3. Finally, the revisions the entity made to its transmission planning procedure were limited to one subsection and included only clarifying statements as opposed to additional interconnection voltage requirements. Specifically, the entity clarified that it did not impose any specific voltage MW or MVAR requirements on generation facilities only that "a generator developer connecting to the [the entity's] Transmission shall supply electricity to the Points of Interconnections at a nominal voltage of 115, 230, or 500kV." The entity included the requirement that generator developers only connect to its transmission at nominal voltages of 115, 230, or 500 kV in its transmission planning procedure prior to the issue with FAC-001-0 R2.1.3.	The entity submitted a letter to Reliability*First* describing the following mitigating actions it took to address the issue of FAC-001-1 R2.1.3. Shortly following the Reliability*First* compliance audit, the entity approved revisions to its transmission planning procedure, which the entity posted to its public website. The entity limited its revisions to the section dealing with interconnection voltage and MW and MVAR capacity requirements. The entity's revisions do not alter its interconnection requirements, but rather clarifies that "Points of Interconnections for all transmission facilities connected to BGE shall be at a nominal voltage or 115, 230, or 500kV," and that "[The entity] does not invoke any additional Voltage, MW and/or MVAR requirements on transmission facilities unless specific interconnection evaluations reveal a need to do so." The entity completed its mitigation activities, as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100744	VAR-002-1	R1	The entity submitted a Self-Report to Reliability*First* identifying a possible issue with VAR-002-1 R1. During an internal review, the entity determined that it failed to operate its automatic voltage regulators (AVRs) in automatic voltage control mode for the five generating units at a generating station, as required by VAR-002-1 R1 since the entity first operated the AVRs in VAR mode. Pursuant to the entity's interpretation of manufacturer information, the entity operated the AVRs in automatic operation with VAR control mode selected (VAR mode). The entity believed that VAR mode maintained a constant generator terminal voltage. Upon further internal review and the receipt of a clarifying technical information letter from the manufacturer, the entity realized that operating in VAR mode was not equivalent to operating the AVRs in automatic voltage control mode pursuant to VAR-002-1 R1. The entity's AVR control screens provided three modes of control: OFF, PF, or VAR. The entity thought that its generating units were operating in automatic voltage control when in VAR mode, but later learned from the technical information letter that to in order to operate its AVRs in automatic voltage control mode, the AVRs had to be in the OFF mode. Due to this misinterpretation of manufacturer information, the entity failed to notify its Transmission Operator that the five generating units were operating in VAR mode. Reliability*First* determined that the entity had an issue with VAR-002-1 R1 by failing to operate each generator connected to the interconnected transmission system in automatic voltage control mode.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that, although the AVRs were not in automatic voltage control mode, they remained in VAR mode, which would allow them to respond to any voltage changes. An AVR in VAR mode will respond to maintain VARs at a fixed value. If system voltage decreases, a voltage regulator in VAR mode will sense the decrease in VAR output and will adjust the generator excitation to restore the generator output to a stable value. In addition, the entity attests that the entity has followed any directive given by the Transmission Operator regarding the entity's generating station voltage schedule.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First* . The entity changed the control modes on the AVRs at the five generating units to automatic voltage control mode and disseminated the information learned from the issue throughout the company. In addition, the entity retrained all control room operators on proper AVR control mode operation. The entity also revised plant operating procedures to clarify the necessary usage of automatic voltage control mode unless requested to do otherwise by the Balancing Authority or Transmission Operator. Furthermore, the entity modified its software to require its operators to make two distinct operational selections in order to shift the AVRs out of automatic voltage control mode. The entity completed its mitigation activities, as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100745	VAR-002-1	R3	The entity submitted a Self-Report to Reliability*First* identifying a possible issue with VAR-002-1 R3. During an internal review, the entity determined that it failed to operate its automatic voltage regulators (AVRs) in automatic voltage control mode for five generating units as required by VAR-002-1 R3 since the entity first operated the AVRs in VAR mode. Due to the entity's misinterpretation of manufacturer information, the entity operated the AVRs in VAR control mode selected (VAR mode). Therefore, the entity failed to notify its Transmission Operator that the units were operating in VAR mode. Reliability*First* determined that the entity had an issue with VAR-002-1 R3 by failing to notify its Transmission Operator within 30 minutes of a status change on its AVRs.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated by the fact that, although the AVRs were not in automatic voltage control mode, they remained in VAR mode, which would allow them to respond to any voltage changes. An AVR in VAR mode will respond to maintain VARs at a fixed value. If system voltage decreases, a voltage regulator in VAR mode will sense the decrease in VAR output and will adjust the generator excitation to restore the generator output to a stable value. In addition, the entity attests that the entity has followed any directive given by the Transmission Operator regarding the entity's generating station voltage schedule.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First* . The entity changed the control modes on the AVRs at the five generating units to automatic voltage control mode and disseminated the information learned from the issue throughout the company. In addition, the entity retrained all control room operators on proper AVR control mode operation. The entity also revised plant operating procedures to clarify the necessary usage of automatic voltage control mode unless requested to do otherwise by the Balancing Authority or Transmission Operator. Furthermore, the entity modified its software to require its operators to make two distinct operational selections in order to shift the AVRs out of automatic voltage control mode. The entity completed its mitigation activities, as verified by Reliability*First* .

Attachment A-1

December 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

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 3 (RFC_URE3)	NCRXXXXX	RFC201100770	EOP-008-0	R1; R1.3; R1.5; R1.6	During a compliance audit, Reliability*First* discovered that the entity had a possible issue with EOP-008-0 R1. The entity had in place a contingency plan to continue reliability operations in the event its control center becomes inoperable. Subsequently, the entity had in place a revised contingency plan. The audit team determined that the contingency plan and the revised contingency plan failed to address generation control or logging of significant power system events, as required by EOP-008-0 R1.3. In addition, in the first contingency plan, the entity failed to include procedures and responsibilities for conducting periodic tests, at least annually, to ensure viability of the plan, as required by EOP-008-0 R1.5. The entity also failed to include procedures and responsibilities for providing annual training to ensure that operating personnel are able to implement the contingency plan, as required by EOP-008-0 R1.6. Reliability*First* determined that the entity had an issue with EOP-008-0 R1 by failing to include all necessary information in its contingency plan to continue reliability operations in the event its control center becomes inoperable.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not 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 entity recognized the requirements of EOP-008-0 R1 even though its contingency plan did not make specific statements concerning these requirements. For example, the entity has had a back-up center where it ran tests that balanced generation and demand from the back-up center utilizing Automatic Generation Control (AGC) and logging of events in the senior coordinator's log. In addition, the entity operated from the back-up center at least once per year. The entity did not have to utilize its contingency plan throughout the duration of the issue. The entity conducted periodic tests throughout the year and trained all control staff members in the process. Furthermore, the contingency plan was an interim plan that was in effect for only a short period of time. Since R1.5 and R1.6 require activities that must be done at least annually, the issue with R1.5 and R1.6 for the contingency plan had no practical impact on whether the entity completed these activities annually.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First*. The entity revised its contingency plan to incorporate the required elements under R1.3. Reliability*First* determined that the entity had mitigated R1.5 and R1.6 in the current contingency plan. The entity completed its mitigation activities.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 4 (RFC_URE4) InterPower / AhlCon Partners Limited Partnership [GOP] (IPAC)	NCRXXXXX	RFC2011001092	CIP-003-1	R2; R2.2; R2.3	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered that the entity had a possible issue with CIP-003-1 R2. The CIP senior manager for the entity and its affiliates delegated the authority to perform the CIP senior manager functions that are necessary to ensure compliance with CIP-002 R4 to another individual. The entity's parent company changed the delegated senior manager authority to a different individual. Pursuant to CIP-003-1 R2.2 and R2.3, the entity was required to document that change within thirty calendar days; however, the entity did not document that change until approximately 3 months later. Reliability*First* determined that the entity had an issue with the Standard by failing to document evidence of its senior management delegation change within thirty calendar days of the effective date of the change.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The issue is a documentation error because although the entity did not document the senior manager delegation change within 30 calendar days, the senior manager delegate did begin performing all delegated senior manager functions. In addition, the entity has no Critical Cyber Assets.	In order to mitigate the issue, the entity documented the senior manager delegation change. During the compliance audit, Reliability*First* verified the completion of the entity's mitigating actions.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 5 (RFC_URE5) InterPower / AhlCon Partners Limited Partnership [GOP] (IPAC)	NCRXXXXX	RFC2011001093	CIP-003-1	R2; R2.2; R2.3	Reliability*First* conducted a compliance audit of the entity, during which Reliability*First* discovered that the entity had a possible issue with CIP-003-1 R2. The CIP senior manager for the entity and its affiliates delegated the authority to perform the CIP senior manager functions that are necessary to ensure compliance with CIP-002 R4 to another individual. Subsequently, the entity's parent company changed the delegated senior manager authority to a different individual. Pursuant to CIP-003-1 R2.2 and R2.3, the entity was required to document that change within thirty calendar days; however, the entity did not document that change until approximately 3 months later. Reliability*First* determined that the entity had an issue with the Standard by failing to document evidence of its senior management delegation change within thirty calendar days of the effective date of the change.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The issue is a documentation error because although the entity did not document the senior manager delegation change within 30 calendar days, the senior manager delegate did begin performing all delegated senior manager functions. In addition, the entity has no Critical Cyber Assets.	In order to mitigate the issue, the entity documented the senior manager delegation change. During the compliance audit, Reliability*First* verified the completion of the entity's mitigating actions.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC2011001123	CIP-004-3	R2	The entity self-reported to Reliability*First* a possible issue of CIP-004-3 R2. In the Self-Report, the entity stated that it granted unescorted physical access to Critical Cyber Assets (CCAs) to an employee prior to conducting a personnel risk assessment for that employee and prior to that employee's completion of the entity's cyber security training. Reliability*First* determined that the entity had an issue with CIP-004-3 R2 by failing to train an employee having unescorted physical access to CCAs prior to granting such access to the employee.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although the entity granted the employee with unescorted physical access, the employee was stationed at a remote site and was not aware that the entity had granted this access. The employee made no attempt to nor did the employee enter any Physical Security Perimeters. Additionally, the entity performed a personnel risk assessment for the employee after granting the access and discovered no issues. Finally, the elapsed time from the entity granting access to the entity's discovery and revocation of such access was less than two business days.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First.* The entity updated its access request database to prevent future accidental approvals for authorized cyber or authorized unescorted physical access to CCAs.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 6 (RFC_URE6)	NCRXXXXX	RFC2011001124	CIP-004-3	R3	The entity self-reported to Reliability*First* a possible issue of CIP-004-3 R3. In the Self-Report, the entity stated that it granted unescorted physical access to Critical Cyber Assets (CCAs) to an employee prior to conducting a personnel risk assessment for that employee and prior to that employee's completion of the entity's cyber security training. Reliability*First* determined that the entity had an issue with CIP-004-3 R3 by failing to conduct a personnel risk assessment for an employee, prior to granting the employee authorized unescorted physical access to CCAs.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. Although the entity granted the employee with unescorted physical access, the employee was stationed at a remote site and was not aware that the entity had granted this access. The employee made no attempt to nor did the employee enter any Physical Security Perimeters. Additionally, the entity performed a personnel risk assessment for the employee after granting the access and discovered no issues. Finally, the elapsed time from the entity granting access to the entity's discovery and revocation of such access was less than two business days.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First.* The entity updated its access request database to prevent future accidental approvals for authorized cyber or authorized unescorted physical access to CCAs.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC201100951	FAC-008-1	R1; R1.2; R1.2.2	Reliability*First* conducted a compliance audit of the entity. During the compliance audit, Reliability*First* discovered a possible issue with FAC-008-1 R1 for the entity. The entity's Facility Ratings document is also its Facility Ratings Methodology document, which includes the available methods used when rating equipment; however, the entity failed to designate which rating method it used when rating each of its Facilities, as required by FAC-008-1 R1.2. In addition, the entity failed to address Emergency Ratings in this document as required by FAC-008-1 R1.2.2.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system (BPS). The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity developed Facility Ratings for its BPS facilities and included the available methods for deriving such Ratings. The entity's Facility Ratings Methodology included the statement that "the scope of Ratings addressed shall include, as a minimum, Normal and Emergency Ratings, where applicable," although it failed to specifically state that Normal and Emergency Ratings are the same. In addition, the entity's Facility Ratings did not change when it revised its Facility Ratings Methodology. Furthermore, the entity's facility is designed so that the wind turbine is the most limiting element, which did not change when the entity revised its Facility Ratings Methodology.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First.* The entity revised its Facility Ratings Methodology to include the rating method for each piece of bulk power system equipment and the Emergency Ratings. The entity completed its mitigation activities, as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC201100952	FAC-009-1	R1	Reliability*First* conducted a compliance audit of the entity. During the compliance audit, Reliability*First* discovered a possible issue with FAC-009-1 R1. Since the entity failed to designate which rating method it used when rating each Facility in its Facility Ratings Methodology, the entity failed to establish Facility Ratings that are consistent with the associated Facility Ratings Methodology.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity developed Facility Ratings for its bulk power system facilities and included the available methods for deriving such Ratings. In addition, the entity's Facility Ratings did not change when the entity revised its Facility Ratings Methodology. Furthermore, the entity's facility is designed so that the wind turbine is the most limiting element, which did not change when the entity revised its Facility Ratings Methodology.	The entity submitted a mitigation plan, in which it memorialized the actions it took to address the issue, to Reliability*First* . The entity revised its Facility Ratings Methodology to include the rating method for each piece of bulk electric system equipment. The entity reviewed all facilities rated and confirmed that the Ratings were consistent with the Facility Ratings Methodology. The entity completed its mitigation activities, as verified by Reliability*First* .
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 7 (RFC_URE7)	NCRXXXXX	RFC201100954	PRC-005-1	R1; R1.1	Reliability*First* conducted a compliance audit of the entity. During the compliance audit, Reliability*First* discovered a possible issue with PRC-005-1 R1.1. The entity failed to designate the basis that applies to each Protection System device in its Protection System maintenance and testing program. This issue included all of the entity's Protection System devices.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity maintained and implemented its Protection System maintenance and testing program for all of its 105 Protection System devices. Furthermore, the entity did not change any of its program's maintenance and testing intervals when it revised its Protection System maintenance and testing program to include a specific designation as to which basis applies to which Protection System device. The entity conducted maintenance and testing in accordance with its Protection System maintenance and testing program throughout the duration of the issue. Furthermore, SCADA generates visual alarms upon activation of any substation circuit breaker, and the entity has backup and redundant protection in place for its relays.	The entity revised its Protection System maintenance and testing program to include the basis applied to the maintenance and testing interval for each Protection System device. The entity completed its mitigation plan as verified 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
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 7 (RFC_URE7) EcoGrove Wind, LLC (EcoGrove)	NCRXXXXX	RFC2011001210	CIP-001-1a	R1	The entity self-certified an issue with CIP-001-1a R1, R2, R3 and R4. The entity failed to have procedures in place for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection, as required by CIP-001-1a R1.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity trained its site personnel and operational personnel to recognize and report any sabotage event or potential sabotage event. At all relevant times, the entity maintained an emergency contact list that included local authorities' contact information.	During the compliance audit, ReliabilityFirst reviewed the entity's current sabotage reporting procedure. ReliabilityFirst verified, as part of this review, that the current sabotage reporting procedure illustrates that the entity conducted and completed mitigating activities for the issue. The entity put in place a procedure for the recognition of and for making their operating personnel aware of sabotage events on its facilities.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 7 (RFC_URE7) EcoGrove Wind, LLC (EcoGrove)	NCRXXXXX	RFC2011001211	CIP-001-1a	R2	The entity self-certified an issue with CIP-001-1a R1, R2, R3 and R4. The entity failed to have in place procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection, as required by CIP-001-1a R2.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity trained its site personnel and operational personnel to recognize and report any sabotage event or potential sabotage event. At all relevant times, the entity maintained an emergency contact list that included local authorities' contact information.	During the compliance audit, ReliabilityFirst reviewed the entity's current sabotage reporting procedure. ReliabilityFirst verified, as part of this review, that the current sabotage reporting procedure illustrates that the entity conducted and completed mitigating activities for the issue. The entity put in place a procedure for the communication of information concerning sabotage events to appropriate parties in the interconnection.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 7 (RFC_URE7) EcoGrove Wind, LLC (EcoGrove)	NCRXXXXX	RFC2011001212	CIP-001-1a	R3	The entity self-certified an issue with CIP-001-1a R1, R2, R3 and R4. The entity failed to provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events, as required by CIP-001-1a R3.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity trained its site personnel and operational personnel to recognize and report any sabotage event or potential sabotage event. At all relevant times, the entity maintained an emergency contact list that included local authorities' contact information.	During the compliance audit, ReliabilityFirst reviewed the entity's current sabotage reporting procedure. ReliabilityFirst verified, as part of this review, that the current sabotage reporting procedure illustrates that the entity conducted and completed mitigating activities for the issue. The entity provided its operating personnel with sabotage response guidelines, including personnel to contact for reporting disturbances due to sabotage events.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 7 (RFC_URE7) EcoGrove Wind, LLC (EcoGrove)	NCRXXXXX	RFC2011001213	CIP-001-1a	R4	The entity self-certified an issue with CIP-001-1a R1, R2, R3 and R4. The entity failed to establish communications contacts with local Federal Bureau of Investigation officials and develop reporting procedures as appropriate to its circumstances, as required by CIP-001-1a R4.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not serious or substantial, risk to the reliability of the bulk power system. The risk posed by the foregoing facts and circumstances was mitigated by the following factors. The entity trained its site personnel and operational personnel to recognize and report any sabotage event or potential sabotage event. At all relevant times, the entity maintained an emergency contact list that included local authorities' contact information.	During the compliance audit, ReliabilityFirst reviewed the entity's current sabotage reporting procedure, which has been in place since October 5, 2010. ReliabilityFirst verified, as part of this review, that the current sabotage reporting procedure illustrates that the entity conducted and completed mitigating activities for the issue. The entity established communications contacts with the county sheriff and the FBI, and the entity has a procedure directing its staff to provide sabotage event information.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 8 (RFC_URE8) NRG Rockford LLC	NCRXXXXX	RFC2011001188	CIP-002-1	R3	ReliabilityFirst conducted a compliance audit and discovered a possible issue with CIP-002-1 R3 for the entity. The entity determined, through annual application of its risk-based assessment methodology (RBAM), that it had no Critical Assets, and developed a null list reflecting that fact as required by CIP-002-1 R2; however, the entity did not create a null list to reflect the fact that it had no Critical Cyber Assets (CCAs), as required by CIP-002-1 R3.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not 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 entity determined through the annual application of its RBAM that it had no Cyber Assets and no CCAs. The issue is a documentation errors because the entity did not create a null list of CCAs, in addition to the null list it created for Cyber Assets.	The entity submitted a letter certifying that it completed the necessary mitigating activities, along with evidence of completion, to ReliabilityFirst. Specifically, the entity provided ReliabilityFirst with a copy of its null list of CCAs, which documents that it has no CCAs.
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 8 (RFC_URE8) NRG Rockford LLC	NCRXXXXX	RFC2011001189	CIP-002-1	R4	ReliabilityFirst conducted a compliance audit of the entity and discovered a possible issue with CIP-002-1 R4. The entity did not annually approve its Critical Cyber Assets (CCAs) list (even if the list is null) as required by CIP-002-1 R4, because it never developed a null list of CCAs pursuant to CIP-002-1 R3.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal, not 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 entity determined through the annual application of its RBAM that it has no Cyber Assets and no CCAs. This issue is a documentation error because the entity did not create a null list of CCAs, in addition to the null list it created for Cyber Assets, therefore, the entity could not annually approve a null list of CCAs.	The entity submitted a letter certifying that it completed the necessary mitigating activities, along with evidence of completion, to ReliabilityFirst. Specifically, the entity provided ReliabilityFirst with a copy of its null list of CCAs, which the entity will approve annually. ReliabilityFirst reviewed the evidence the entity submitted, and determined that the entity successfully completed all mitigating actions necessary to resolve the issue of CIP-002-1 R4.

Attachment A-1

December 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

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 9 (RFC_URE9) NRG Rockford II LLC	NCRXXXXX	RFC2011001190	CIP-002-1	R3	Reliability*First* conducted a compliance audit and discovered a possible issue with CIP-002-1 R3 for the entity. The entity determined, through annual application of its risk-based assessment methodology (RBAM), that they have no Critical Assets, and developed a null list reflecting that fact as required by CIP-002-1 R2; however, the entity did not create a null list to reflect the fact that it has no Critical Cyber Assets (CCAs), as required by CIP-002-1 R3.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not 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 entity determined through the annual application of its RBAM that it has no Cyber Assets and no CCAs. This issue is a documentation error because the entity did not create a null list of CCAs, in addition to the null list it created for Cyber Assets.	The entity submitted a letter certifying that they completed the necessary mitigating activities, along with evidence of completion, to Reliability*First*. Specifically, the entity provided Reliability*First* with a copy of its null list of CCAs, which documents that the entity has no CCAs.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 9 (RFC_URE9) NRG Rockford II LLC	NCRXXXXX	RFC2011001191	CIP-002-1	R4	Reliability*First* conducted a compliance audit of the entity and discovered a possible issue with CIP-002-1 R4. The entity did not annually approve its Critical Cyber Assets (CCAs) list (even if the list is null) as required by CIP-002-1 R4, because it never developed a null list of CCAs pursuant to CIP-002-1 R3.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal, not 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 entity determined through the annual application of its RBAM that it has no Cyber Assets and no Critical Cyber Assets (CCAs). This issue is a documentation error because the entity did not create a null list of CCAs, in addition to the null list it created for Cyber Assets, therefore, the entity could not annually approve a null list of CCAs.	The entity submitted a letter certifying that it completed the necessary mitigating activities, along with evidence of completion, to Reliability*First*. Specifically, the entity provided Reliability*First* with a copy of its null list of CCAs, which the entity will approve annually. Reliability*First* reviewed the evidence the entity submitted, and determined that the entity successfully completed all mitigating actions necessary to resolve the issue of CIP-002-1 R4.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1)	NCRXXXXX	SERC201000583	VAR-002-1	R1	SERC_URE1 self-reported that its generators operated in VAR mode instead of automatic voltage control mode without notifying its Transmission Operator (TOP), as required. A SERC_URE1 vendor released a technical letter indicating that the labeling on certain Automatic Voltage Regulators (AVR) may be misleading. The AVR can be operated in three modes — OFF, VAR, or Power Factor. The technical letter explained that the "OFF" position indicates that the AVR is operating in automatic voltage control mode and recommended that customers consider changing the label from "OFF" to "Voltage Control" to more accurately reflect the generator control mode. After receiving the technical letter, SERC_URE1 surveyed its plants and determined that its plant had been operating in VAR mode. As a result of its assessment, SERC staff determined that SERC_URE1 was in violation of VAR-002-1 R1 because its generators were operating in a mode other than automatic voltage control without notifying its TOP.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. The plant had not experienced any voltage-related reliability issues and had met its voltage schedules from August 2, 2007 through October 31, 2009, which was the last month the plant had been on-line before switching the AVRs from VAR mode to automatic voltage control mode; and 2. When SERC_URE1 operated, the AVRs were in Auto and controlling VAR mode, which should have allowed the plant to respond to support the BPS, if required.	SERC staff verified that SERC_URE1 completed the following actions: 1. Reviewed NERC reporting procedures and generator start-up procedures with all central control room operators; 2. Revised plant operating procedures regarding AVR modes of operation; 3. Changed the AVR control labeling; and 4. Installed an alarm function to notify operators when the AVR is not in automatic voltage control mode.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC2011008322	FAC-008-1	R1	The SERC audit team discovered a possible violation of FAC-008-1 R1.2.1 stating that SERC_URE2 did not address series and shunt compensation devices in its Facility Rating Methodology (FRM). SERC_URE2's FRM states that SERC_URE2 has an agreement with [Utility A] to use [Utility A]'s procedure. [Utility A]'s procedure, which was provided to SERC staff after the audit, addresses all of the Requirements of the Standard. Therefore, SERC_URE2 was found to be compliant beginning on the date the document became effective. After further examination, SERC staff discovered that SERC_URE2's previous FRM only addressed the generator, which is the limiting element. It did not address the scope of equipment or normal and emergency ratings as required by R1.2. This represents a gap in compliance for FAC-008.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Both of SERC_URE2's FRMs were designed to reflect the most limiting element, the generator. 2. SERC_URE2 operates electric generating units that are connected to [Utility A's] Transmission Grid. SERC_URE2 owns no transmission lines. 3. SERC_URE2 does not own series or shunt compensation devices.	SERC staff verified that SERC_URE2 revised its FRM to meet all of the Requirements of the Standard.

Attachment A-1

December 30, 2011 Public - Find Fix and Track Informational Filing of Remediated Issues Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

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	SPP201000235	CIP-002-1	R3	During a Spot Check, SPP RE's CIP audit team discovered that SPP RE_URE1's Critical Cyber Asset (CCA) list contained substantive errors, indicating an issue with this Standard. SPP RE_URE1 had incorrectly classified a host integration server as a CCA. In addition, several systems that were shown to be out-of-service on the prior year's CCA list were shown back in service on the next year's CCA list, even though those systems remained out of service.	SPP RE determined that SPP RE_URE1's issue with CIP-002-1 R3 did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) and posed only a minimal risk to the BPS. SPP RE_URE1's error to the CCA list was that it included an additional asset rather than omitted an asset that should have been deemed a CCA. Additionally, no "out of service" CCAs listed on the CCA "in-service" list was ever actually put back into service between the two years. SPP RE determined that this was a documentation issue only. As such, there were no CCAs that were left unprotected, and the risk to the BPS was minimal.	SPP RE_URE1 re-assessed its CCA list and removed the host integration server and other systems shown as out-of-service on the prior year's CCA list and had its chief security officer approve the new list. This issue was assigned NERC Mitigation Plan ID MIT-08-2747. SPP RE_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP RE_URE2)	NCRXXXXX	SPP201000327	CIP-004-1	R2 (R2.1, R2.2.1)	During a Spot Check, SPP RE determined that SPP RE_URE2 had an issue with CIP-004-1 R2.1 and R2.2.1. Regarding R2.1, 3.2% of randomly sampled personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) were not trained within 90 days of such authorization. An SPP RE Enforcement's subsequent survey of 100% of SPP RE_URE2's employees with authorized cyber or authorized unescorted physical access revealed that a total of 4% of SPP RE_URE2's entire company had not received training within 90 days of being granted access. Regarding R2.2.1, although SPP RE_URE2's EMS/SCADA vendor conducted its own cyber security training for its support personnel, two year's of annual training did not include the proper use of CCAs, as required by this Standard.	SPP RE has determined that SPP RE_URE2's issue with CIP-004-1 R2 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Regarding R2.1, the 4% of individuals who had not received training within 90 days from authorized access were trusted employees with no disciplinary actions who had received the required cyber security training by early in 2010. This was confirmed by Personnel Risk Assessments (PRAs) that were being conducted during this time by SPP RE_URE2. Regarding R2.2.1, while the EMS/SCADA vendor was not trained on the proper uses of SPP RE_URE2's CCAs, the small group of vendor support personnel received comprehensive training on CIP Standards and work in a position that requires technical knowledge inclusive of cyber security best practices. As such, they fully understood the implications of their access to SPP RE_URE2's CCAs.	Regarding R2.1, as early in 2010, SPP RE_URE2 had trained all personnel with authorized cyber or authorized unescorted physical access to CCAs. SPP RE_URE2 also implemented a NERC CIP flag in its HR system that keeps track of all personnel with authorized access to SPP RE_URE2's CCAs. This new system allows SPP RE_URE2 to cross reference training records in order to verify that all affected personnel has received cyber security training within required intervals. Regarding R2.2.1, SPP RE_URE2 issued its EMS/SCADA vendor that addresses the proper use of its CCAs. Vendors support personnel must now acknowledge reading and understanding this summary before being granted cyber access. This issue was assigned NERC Mitigation Plan ID MIT-08-3014. SPP RE_URE2 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 3 (SPP RE_URE3)	NCRXXXXX	SPP201100664	CIP-007-3	R5.3	SPP RE_URE3 Self-Reported an issue with CIP-007-1 R5.3. SPP RE_URE3 submitted three Technical Feasibility Exception (TFE) requests, regarding its Oracle database server and compliance with CIP-007-1 R5.3.1, R5.3.2, and R5.3.3. SPP RE approved the TFE requests. The TFEs were necessary because the Oracle database server had a hardcoded password that made it operationally infeasible to comply with CIP-007-1 R5.3. SPP RE_URE3 had anticipated that it would resolve its issues with the database password before its TFEs expired, with the resolution having the ability to comply with all requirements of CIP-007-3 R5.3. However, in mid-2011, SPP RE_URE3 had not yet resolved its database password issue, and the three TFEs pertaining to CIP-007-3 R5.3 expired. SPP RE_URE3 filed new TFEs for CIP-007-3 R5.3.	SPP RE has determined that SPP RE_URE3's issue with CIP-007-3 R5.3 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP RE_URE3 allowed the three TFEs pertaining to CIP-007-3 R5.3 to expire, SPP RE_URE3 continued the compensating and mitigating measures described in its TFEs. Namely, SPP RE_URE3's database user password is only accessible to personnel with a "need to know" status, and all personnel with a "need to know" status have attended security awareness training and have had background checks performed. Additionally, all scripts containing the password are within a secured ESP. Furthermore, the gap between the expiration of the TFEs that were filed and the date that SPP RE_URE3 resubmitted TFEs for the Oracle database password lasted only about one month. Lastly, SPP RE_URE3's resubmitted TFEs with the same compensating and mitigating measures that it had in place with the TFEs filed and the same measures it had continued to perform during the one-month gap in which it did not have valid TFEs.	SPP RE_URE3 filed another TFE to cover the period between the newly filed TFE request and the date of implementation of its new SCADA system and historian server. This issue was assigned NERC Mitigation Plan ID SPPMIT005948. SPP RE_URE3 certified that mitigation was complete.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201100381	CIP-002-3	R1	This issue was discovered through an Audit. Texas RE determined that for the audit period, Texas RE_URE1's Risk-Based Assessment Methodology did not consider applicable assets of its Qualified Scheduling Entity. The Qualified Scheduling Entity was under contract to perform communications with the Reliability Coordinator and the Balancing Authority on behalf of Texas RE_URE1.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because Texas RE_URE1 did not have any Critical Assets. Further, Texas RE_URE1 found no Critical Assets after it modified and implemented its Risk-Based Asset Methodology to address this issue. Texas RE_URE1's Risk-Based Asset Methodology was very thorough and the exclusion of the Qualified Scheduling Entity communications was based on the inability of those communications to directly control Texas RE_URE1's generation assets because their control resides within Texas RE_URE1's control rooms.	Texas RE_URE1 mitigated the issue by modifying, approving and implementing its Risk-Based Assessment Methodology to specifically consider the control room functions contracted away to its Qualified Scheduling Entity.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE201100352	CIP-003-2	R3	A Self-Report addressing this issue was submitted to Texas RE, after a notification of Texas RE's Audit was sent to Texas RE_URE2. Texas RE_URE2 reported that it did not properly document an exception to its Cyber Security Policy and that the exception was related to the failure to perform monthly ports and services checks according to Texas RE_URE2's Desk Procedures and CIP-007. Texas RE determined that the discovery method for this issue was an Audit.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because the check of the ports and services that was not performed according to CIP-007, is also required to be performed annually by the Reliability Standards. Texas RE_URE2's Desk Procedures require more frequent checks than the annual check required by the Standard. Texas RE_URE2 restarted its monthly checks, which are required by its Desk Procedures, before the annual check would have been due.	The required exception document has been completed and approved. Additionally, the management of the responsible department provided additional awareness education and strengthened the language in the Texas RE_URE2's procedure documents regarding the process for obtaining an exception when Texas RE_URE2 is unable to conform to its Cyber Security Policy.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (Texas RE_URE2)	NCRXXXXX	TRE201100350	CIP-002-2	R3	During an Audit, Texas RE found four devices on Texas RE_URE2's Critical Cyber Asset (CCA) list to be outside of the Physical Security Perimeter (PSP). Texas RE further determined that the four devices did not belong to the CCA list but were mistakenly added to the list, in violation of this Standard.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because the four devices in question were part of a test platform that was not part of any Electronic Security Perimeter (ESP). The devices were mistakenly added to the CCA list and the annual review of the CCA list had not yet occurred for that year.	The CCA list was reviewed and the test platform devices were removed from it.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (Texas RE_URE3)	NCRXXXXX	TRE201000226	CIP-006-1	R4.3	Texas RE_URE3 Self-Reported that it had an issue with CIP-006-1 R4.3 on two specific incidents because Texas RE_URE3 failed to implement manual logging controls for personnel that were granted escorted access to established Physical Security Perimeters (PSPs).	The First Instance: This issue did not pose a serious or substantial risk and had a moderate risk to the bulk power system (BPS) because although there was an issue with proper logging, the employee who entered the PSP of the transmission dispatch center had previously completed background checks. The Second Instance: This issue did not pose a serious or substantial risk and posed a moderate risk to the BPS because although there was an issue with proper logging, on the Second Instance, an IT contractor entering the telecommunications room at the system operator building without having been properly logged into the facility had completed required cyber security training, had a clear background check, and had been granted authorized physical access to the telecommunications room at the same system operator's building. Further, the contractor was escorted by an employee during the entire period.	Email communication was issued to remind Texas RE_URE3 staff of the visitor physical access requirements and processes. In addition, CIP Facility Visitor Log requirements training material and discussion guide were given to staff.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (Texas RE_URE4)	NCRXXXXX	TRE201100268	CIP-009-2	R1.1	Texas RE discovered an issue with this Standard during a Spot Check. Texas RE_URE4's Recovery Plans did not specifically address varying duration and severity levels that would activate the recovery plan(s). Texas RE found that Texas RE_URE4's recovery plan discusses all exercises and procedures to recover specific Critical Cyber Assets (CCAs) including steps to follow in an event of emergency. The procedure specified that failed cyber assets be replaced immediately and all relevant contact information of personnel necessary for recover specific failures was also included in the procedure. Texas RE_URE4 modified its procedure to include varying duration and severity after Texas RE_URE4 was notified of this finding during a certification process.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because Texas RE_URE4's CCA recovery plan was in place and was being annually reviewed. Moreover, specific CCA device failures and the procedure to recover them was specified in detail in the recovery plan. It was specified that the failed device will be repaired or replaced immediately and brought back to service. The notification procedure and contact information of personnel to contact for specific failures was also mentioned in the procedures.	This issue was mitigated in a later recovery plan document once Texas RE_URE4 was notified of the limitations during the certification process. The new Recovery Plans for CCAs address varying duration and severity that would activate the recovery plan(s).
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 5 (Texas RE_URE5) ANP Funding I, LLC (ANP)	NCRXXXXX	TRE201100338	CIP-002-3	R2	Texas RE discovered this issue during a Spot Check. Texas RE_URE5's current risk-based assessment methodology included a Critical Asset (CA) and Critical Cyber Asset (CCA) list that addressed the current requirement. Texas RE requested an earlier version of the risk-based assessment, CA and CCA list. Texas RE_URE5 failed to provide these documents, indicating an issue with this Standard but Texas RE_URE5's procedure and CIP Assessment Methodology required an annual review and assessment of CA and CCA's.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because Texas RE_URE5 did not and still does not have any CAs and CCAs following the compliance date.	This issue was mitigated when Texas RE_URE5's Critical Asset Methodology (RBAM), CA and CCA list were approved by the senior manager and the application of RBAM resulted in no CA or CCA identification.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 5 (Texas RE_URE5) ANP Funding I, LLC (ANP)	NCRXXXXX	TRE201100339	CIP-002-3	R3	Texas RE discovered this issue during a Spot Check. Texas RE_URE5's current risk-based assessment included a Critical Asset (CA) and Critical Cyber Asset (CCA) list that addressed this Standard's requirement. Texas RE requested an earlier version of Texas RE_URE5's risk-based assessment, and CA and CCA lists but Texas RE_URE5 did not provide any, indicating an issue with this Standard. However, Texas RE_URE5's procedure and CIP Assessment Methodology required an annual review and assessment of CA and CCA's.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because Texas RE_URE5 did not and still does not have any CAs or any CCAs following the compliance date.	This issue was mitigated when Texas RE_URE5's Critical Asset Methodology (RBAM), CA and CCA list were approved by the senior manager and the application of RBAM resulted in no CA or CCA identification.

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 5 (Texas RE_URE5) ANP Funding I, LLC (ANP)	NCRXXXXX	TRE20100340	CIP-002-3	R4	Texas RE discovered this issue at a Spot Check. Texas RE determined that Texas RE_URE5 had an issue with CIP-002-3 R4 because Texas RE_URE5's Critical Asset Methodology (RBAM) was not approved by the Senior Manager nor it was delegated to anyone else to approve it. CA and CCA list were approved by the Senior Manager.	This issue did not pose a serious or substantial risk and posed a minimal risk to the bulk power system because Texas RE_URE5 did not and does not have any Critical Assets or any Critical Cyber Assets. Moreover, RBAM existed but was not officially signed off by the Senior Manager. The RBAM, CA and CCA list were approved by Senior Manager within the Standard's annual requirement.	This issue was mitigated when RBAM, CA and CCA list were approved by the Senior Manager and the application of RBAM resulted in no CA or CCA identification.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 6 (Texas RE_URE6)	NCRXXXXX	TRE201100293	FAC-009-1	R1	Texas RE_URE6 Self-Reported that while reviewing the NERC Alert "Considerations of Actual Field Conditions in Determination of Facility Ratings", Texas RE_URE6 discovered that the facility ratings for Texas RE_URE6 did not include an equipment rating for Texas RE_URE6's generation interconnection line. Upon further review, Texas RE_URE6 also became aware that generation interconnection lines should be included within the scope of equipment from which the facility's rating were established. This line was omitted from the Texas RE_URE6's Facility Rating Methodology and ties the plant to another entity's transmission substation.	Texas RE determined that this issue did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system. The generator interconnection transmission line that was not included in the implementation of Texas RE_URE6's Facility Rating Methodology was not the most limiting element of the Facility. Proper coordination appears to have occurred between Texas RE_URE6 and the other entity after review of the Interconnection Agreement. Relay settings were reviewed and did not need modification and ERCOT ISO was being informed of the line's rating and status during the issue period. No disturbances occurred on the transmission line during the period of non-compliance.	Texas RE_URE6 has enhanced its Facility Rating Methodology to specifically include generation tie lines and updated the Facility ratings. An updated Facilities rating sheet was provided for the transmission line. Texas RE_URE6 also provided a screen shot of the submission to ERCOT that showed the facility ratings and the most limiting factor of the facility.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 7 (Texas RE_URE7)	NCRXXXXX	TRE201100292	FAC-009-1	R1	Texas RE_URE7 Self-Reported that while reviewing the NERC Alert "Considerations of Actual Field Conditions in Determination of Facility Ratings", it discovered that the facility ratings for Texas RE_URE7 did not include an equipment rating for Texas RE_URE7's generation interconnection line. Upon further review, Texas RE_URE7 also became aware that generation interconnection lines were to be included among the scope of equipment from which the facility's rating should be established. The line was omitted from the Texas RE_URE7 Facility Rating Methodology and ties the plant to another entity's transmission substation. Based on the record, SPP RE determined that these facts indicate an issue with 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. The generator interconnection transmission line that was not included in the implementation of Texas RE_URE7's Facility Rating Methodology was not the most limiting element of the Facility. Proper coordination occurred between Texas RE_URE7 and the other entity after review of the Interconnection Agreement. Relay settings were reviewed and did not need modification and ERCOT was being informed of the line's rating and status during the issue period. No disturbances occurred on the transmission line during the period of non-compliance.	Texas RE_URE7 has enhanced their Facility Rating Methodology to specifically include generation tie lines and updated the Facility ratings. An updated Facilities rating sheet was provided for the transmission line. Texas RE_URE7 also provided a screen shot of the submission to ERCOT that showed the facility ratings and the most limiting factor of the facility.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201103030	CIP-004-3	R4	WECC_URE1 submitted a Self-Report to WECC. A WECC Subject Matter (SME) contacted WECC_URE1 to discuss its Self-Report. According to the WECC SME, during the discussion WECC_URE1 stated that it failed to review one out of its five access list types in the first quarter of 2011. WECC_URE1's five access lists are Physical Card key, Physical hard key, electronic supervisory control and data acquisition (SCADA), Physical Access Control Systems, and Access Database. The access list WECC_URE1 failed to review is the "Electronic SCADA" access list.	WECC determined this issue posed minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). While failure to maintain a list of personnel with logical and/or physical access to Critical Cyber Assets (CCAs) could allow malicious logical and/or physical access to CCAs which could compromise the security of such assets essential to the BPS, thereby disrupting the reliable operation of the BPS, in this instance, WECC_URE1 stated that all individuals with access to CCAs had current personnel risk assessments and CIP training, and all CCAs were located in a Physical Security Perimeter and Electronic Security Perimeter and provided the protections of CIP-006 and CIP-005.	WECC_URE1 performed the second and third quarter reviews of 2011.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201103036	CIP-004-3	R4	WECC_URE2 submitted a Self-Report to WECC. A WECC Subject Matter (SME) contacted WECC_URE2 to discuss its Self-Report. According to the WECC SME, during the discussion WECC_URE2 stated that it failed to review one out of its five access list types in the first quarter of 2011. WECC_URE2's five access lists are Physical Card key, Physical hard key, electronic supervisory control and data acquisition (SCADA), Physical Access Control Systems, and Access Database. The access list WECC_URE2 failed to review is the "Electronic SCADA" access list. In addition, WECC_URE2 stated that on one occasion it failed to update its access list within seven days of an individual no longer requiring authorized access and failed to revoke access and update is access list for a contractor who no longer required access to Critical Cyber Assets.	WECC determined this issue posed minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). While failure to maintain a list of personnel with logical and/or physical access to Critical Cyber Assets (CCAs) could allow malicious logical and/or physical access to CCAs which could compromise the security of such assets essential to the BPS, thereby disrupting the reliable operation of the BPS, in this instance, WECC_URE2 stated that all individuals with access to CCAs had current personnel risk assessments and CIP training, and all CCAs were located in a Physical Security Perimeter and Electronic Security Perimeter and provided the protections of CIP-006 and CIP-005.	WECC_URE2 performed the second and third quarter reviews of 2011.

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 3 (WECC_URE3)	NCRXXXXX	WECC201103049	MOD-001-1a	R8	WECC_URE3 submitted a Self-Report to WECC. WECC_URE3 had received a month-ahead planned outage notification that required WECC_URE3 to recalculate its monthly Available Transfer Capability (ATC). Pursuant to MOD-001-1 R8.3, WECC_URE3 had one week to recalculate its monthly ATC. WECC_URE3 did not recalculate its monthly ATC until 16 calendar days beyond the date specified in the Reliability Standard.	WECC determined this issue posed minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). While failing to update an ATC may cause a Transmission Service Provider to lose awareness of its available system capacity, including flows within its system or in neighboring systems, in this case WECC_URE3's Grid Operations staff was aware of the planned outage and WECC_URE3 calculated its ATC prior to the outage taking effect. There is no evidence indicating WECC_URE3 was operating its system with an inaccurate ATC. WECC_URE3 did not meet the timing requirements outlined in MOD-001-1a R8, however WECC_URE3 appropriately calculated its ATC prior to the planned outage.	WECC_URE3 recalculated its ATC prior to the planned outage.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA201100125, NCEA201100126	CIP-007-1	R4, R4.1, R4.2	NCEA_URE1 submitted a Self-Report to NCEA stating that its Hewlett-Packard (HP) Printers and Multi Function Printers (MFPs) do not have the capabilities to install anti-virus or malicious software prevention tools. Such software is neither provided by HP nor is it available from third parties.	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 files including software updates are scanned for anti-virus and anti-malware on other systems prior to entering the Electronic Security Perimeter (ESP). Software updates are also verified by comparing to the manufacturer's (hash) files when available. These printers were not included on the initial list of TFEs submitted by NCEA_URE1.	The TFE was submitted to NCEA and approved. NCEA_URE1 is unaware of similar devices that have anti-virus or anti-malware capabilities. NCEA_URE1 will continue to research the market for similar devices that will meet these requirements of these devices. All files including software updates are scanned for anti-virus and anti-malware on other systems prior to entering the ESP. Software updates are also verified by comparing to the manufacturer's (hash) files when available.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA201100127	CIP-007-1	R5.3	NCEA_URE1 submitted a Self-Report to NCEA stating that its Hewlett-Packard (HP) Printers and Multi Function Printers (MFPs) are not capable of implementing password controls for Administrator accounts as required by NERC standards.	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 access to the printers is only available to users on the administrative network which is strictly controlled. These printers were not included on the initial list of TFEs submitted by NCEA_URE1.	The TFE was submitted to NCEA and approved. Access to the printers is only available to users on the administrative network which is strictly controlled. The compensating and/or mitigating measures have been fully implemented.
NERC Compliance Enforcement Authority (NCEA)	Unidentified Registered Entity 1 (NCEA_URE1)	NCRXXXXX	NCEA201100128	CIP-007-3	R6.3	NCEA_URE1 submitted a Self-Report to NCEA stating that the Event Logging in Hewlett-Packard (HP) LaserJet printers T610 plotters is limited to device and printing errors. It does not provide security event logging for authentication errors, setting changes, or other security related events. This issue was discovered as part of NCEA_URE1's ongoing process to review its compliance with applicable Reliability Standards, it was discovered that these printers did not meet the Requirements for security event logging as required.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because meeting this Requirement is not technically feasible for this entity and NCEA_URE1 has submitted a TFE.	The HP LaserJet printers T610 plotters were disconnected from the Electronic Security Perimeter (ESP) and moved to a secured area network outside of the ESP, where real-time plant data can be amassed on a server that sits between the process and general networks, allowing general users to get any necessary data without having to directly access the system itself. For prevention of future risk, connection to the secured area containing the printers is limited. Firewall policy only allows administration connections to the printers from the administrator's management workstations. All connections to the printers are logged in the firewall.

Document Content(s)