Federal Energy Regulatory Commission
Washington, D.C. 20426

January 20, 2022

FOIA No. FY19-30 (RC12-1)
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 10, 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. RC12-1, 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 RC12-1.

With respect to the remaining identities of UREs contained in RC12-1, 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 RC12-1 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: 2022.01.18 18:56:55 -05'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

RC12-1

Southwest Louisiana Electric Membership Corporation (SLEMCO)-.pdf p.29

Red Hills Wind Project (Red Hills)-.pdf p. 32-33

Rio Grande Electric Co-Op (Rio Grande)-.pdf page 33

Bandera Electric Co Op (Bandera Electric)-.pdf page 34-35

Electric Reliability Council of Texas, Inc. (ERCOT)-.pdf p. 35

Northern California Power Agency (NCPA)-.pdf p. 35

October 31, 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 33 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 82 possible violations[5] of 25 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.

As discussed below, this FFT includes 82 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

enforcement processes for occurrences that posed 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 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 web site 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] the NERC BOTCC reviewed the remediated issues included in this FFT on September 19, 2011. The NERC BOTCC approved the FFT based upon its findings and determinations, the NERC BOTCC's 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 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1120 G Street N.W., Suite 990 Washington, D.C. 20005-3801 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 Regulatory and Corporate Matters North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile 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
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1120 G Street N.W., Suite 990
Washington, D.C. 20005-3801
david.cook@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, D.C. 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
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 OCTOBER 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 NPCC:

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

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

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

FOR RFC:

Robert K. Wargo*
Director of Enforcement 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

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
October 31, 2011

Take notice that on October 31, 2011, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty-three (33) Registered Entities in eight (8) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Attachment A-1

October 31, 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	FRCC201000402	PRC-005-1	R2	The entity self-reported that it had mis-identified one (1 out of a total of 698 Protection System devices) of its relays based upon its Protection System maintenance and testing program to be a microprocessor type relay with a 6-year testing and maintenance interval instead of properly identifying it as a solid state based relay with a 3-year testing and maintenance interval. The entity failed to test the relay within the proper cycle of 3 years, missing the testing by 115 days.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the relay protected a single transmission capacitor bank at one substation. The entity reviewed the classification of all of its relays and found there were no other mis-classifications. No misoperations or system events occurred as a result of the remediated issue. The relay operated correctly during a fault which resulted in taking the capacitor bank out of service.	The entity changed the designation of the relay to the correct type based upon its Protection System maintenance and testing program. The entity performed the required testing and maintenance immediately upon discovery of the mis-classification of the relay.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100417	PRC-001-1	R3	The entity self-reported that it made 51 common timer protection system changes to its relays in a one-month period without coordinating protective system changes with neighboring TOPs and Balancing Authorities (BAs).	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 change to common timers causes the relays to more accurately react to evolving faults thus reducing the fault duration. The change was necessary because it was agreed upon at the FRCC member services level with the other BAs and TOPs prior to changes being made as part of the Florida Event Analysis Team's recommendations. The entity just had no evidence of coordinating prior to the changes having been made.	The entity communicated the protection system changes to the neighboring TOPs and BAs. The entity modified its proper relay settings implementation and coordination procedure to include requirements for coordination of system protection system changes with its neighboring TOPs and BAs.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC200900163	EOP-005-1	R7	The entity was found during a compliance audit that it failed to demonstrate verification of its restoration procedure by actual testing or by simulation for a two-year period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had a documented restoration procedure in place that was used in tabletop training its operators.	The entity's staff verified its restoration procedure using power flow simulation.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC201000379	FAC-008-1	R1	The entity was found during a compliance audit that it did not include in its Facility Ratings Methodology the following; design criteria (R1.3.2), ambient conditions (R1.3.3), operating limitations (R1.3.4), and other assumptions (R1.3.5) for transformers, protective relay devices, breakers and switches for a 17-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating its equipment within manufacturer and design specifications and relay devices, breakers and switches were determined not to be a limiting factor.	The entity revised its Facility Ratings Methodology prior to its audit to include the missing elements as defined within the requirement.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC201000380	FAC-009-1	R1	The entity was found during a compliance audit that it did not include its relay protective devices in its Facility Ratings Methodology for a 29-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating its equipment within manufacturer and design specifications and relay devices were determined not to be a limiting factor.	The entity revised its Facility Ratings prior to the compliance audit to include relay protective devices to meet the requirement.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC201100442	FAC-008-1	R1	The entity self-reported that it did not include in its Facility Ratings Methodology the following; a statement that a Facility Rating shall equal the most limiting applicable Equipment Rating of the individual equipment that comprises that Facility (R1.2); Ratings provided by equipment manufactures' (R1.3.1); ambient conditions (R1.3.3); operating limitations (R1.3.4); and other assumptions (R1.3.5) for a 29-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating its equipment within manufacturer and design specifications. The entity is a waste to energy facility connected at 138 kV with a total generating capacity of less than 75 MW which represents less than 1% (one percent) of the FRCC regional generation.	The entity revised its Facility Ratings Methodology to include the missing elements.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC201100443	FAC-009-1	R1	The entity self-reported that it did not include Ratings for transmission conductors (three - six foot conductors) in its Facility Ratings Methodology for a four-year period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was operating its equipment within manufacturer and design specifications and the three six foot conductors transmission conductors were determined not to be a limiting factor. The entity is a waste to energy facility connected at 138 kV with a total generating capacity of less than 75 MW which represents less than 1% (one percent) of the FRCC regional generation.	The entity revised its Facility Ratings Methodology to include transmission conductors.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 4 (FRCC_URE4)	NCRXXXXX	FRCC201000407	COM-002-2	R2	The entity was found during a compliance audit to have failed to ensure the recipient of a directive (its Generator Operator (GOP)) repeated the information back correctly and acknowledged the response as correct or repeat to resolve any misunderstandings during three occurrences for Mvar adjustments.	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 TOP's instructions were issued in a clear, concise and definitive manner and the directive was limited to the entity's own generators which were continuously monitored and alarmed by the entity's Energy Management System (EMS). The entity is a generating facility connected to the BPS at 230 kV with a total BPS generating capacity of less than 700 MW.	The entity provided training to its TOPs and GOPs in addition to performing a follow-up review of communications to ensure the operators adhered to the requirements of the standard.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 5 (FRCC_URE5)	NCRXXXXX	FRCC200900212	EOP-005-1	R7	The entity was found during a compliance audit that it failed to demonstrate verification of its restoration procedure by actual testing or by simulation for a three-year period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the TOP operates less than 50 miles of 138 kV transmission with no black start capability. The entity had a documented restoration procedure in place that was used in training its operators.	The entity hired a consultant that provided a verification of its restoration procedure using power flow simulation.

Attachment A-1

October 31, 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 6 (FRCC_URE6)	NCRXXXXX	FRCC200900232	EOP-005-1	R7	The entity was found during a compliance audit that it failed to demonstrate verification of its restoration procedure by actual testing or by simulation for a 33-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the TOP operates less than 50 miles of 230 kV transmission with no black start capability. The entity had a documented restoration procedure in place that was used in tabletop training its operators.	The entity's planning engineering staff verified its restoration procedure using power flow simulation.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 7 (FRCC_URE7)	NCRXXXXX	FRCC200900200	EOP-005-1	R7	The entity was found during a compliance audit that it failed to demonstrate verification of its restoration procedure by actual testing or by simulation for a 33-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the TOP operates less than 50 miles of 138 kV transmission with no black start capability. The entity had a documented restoration procedure in place that was used in tabletop training its operators.	The entity hired a consultant that provided a verification of its restoration procedure using power flow simulation.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 8 (FRCC_URE8)	NCRXXXXX	FRCC200900283	EOP-005-1	R7	The entity was found during a compliance audit that it failed to demonstrate verification of its restoration procedure by actual testing or by simulation for a 40-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had a documented restoration procedure in place that was used in training its operators.	The entity hired a consultant that provided a verification of its restoration procedure using power flow simulation.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 9 (FRCC_URE9)	NCRXXXXX	FRCC201100424	FAC-014-2	R5	The entity self-certified that it did not provide its System Operating Limits (SOLs) to those entities with a reliability-related need in 2009. The entity does not have any Interconnection Reliability Operating Limits (IROLs).	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's SOLs would only affect itself and not adjacent Planning Authorities (PAs) and the SOLs had no significant changes in 2009. The entity has a peak load of less than 100 MW is only directly connected to one other Transmission Operator (TOP).	The entity provided the SOLs as required in 2010.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900266	BAL-003-0.1b	R3	The entity self-reported that it did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias. For a 6-hour duration, the entity's AGC was inadvertently operated in Constant Frequency (CF) mode rather than Tie Line Bias (TLB) mode from 00:07 a.m. EST until 05:58 a.m. EST. This was a result of the entity's installation, one day earlier, of an updated AGC resource file which was provided by the software vendor. It was later discovered that the AGC resource file contained a software switch which automatically switched from TLB to CF upon loss of Tie Line telemetry. Tie Line telemetry loss did occur due to a momentary loss of telecommunications at a single site. Throughout the period (from the time of the automatic switch until software support personnel identified cause of inappropriate Area Control Error (ACE) calculation), the AGC calculated ACE did not compare Net Actual and Net Scheduled Interchange. The AGC resource file was promptly corrected upon discovery of the error at 05:58 a.m. EST.	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 improper operational mode of the entity's AGC did not result in undue deviation in the system frequency as there is typically minor movement of AGC during the midnight shift. Also the system frequency component of ACE was being continuously monitored by the entity's Energy Management System (EMS) system operators.	Mitigation included correcting deficiencies in its cyber security change control program to address peer review of application control file changes and further, the entity updated the display of ACE and ACE control process when involving AGC switching. AGC alarms and locations of alarms for SCADA displays for the operators were also included. The entity completed mitigation as verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900267	BAL-005-0.1b	R6	The entity self-reported that it did not operate its Automatic Generation Control (AGC) on Tie Line Frequency Bias. For a 6-hour duration, the entity's AGC was inadvertently operated in Constant Frequency (CF) mode rather than Tie Line Bias (TLB) mode from 00:07 a.m. EST until 05:58 a.m. EST. This was a result of the entity's installation, one day earlier, of an updated AGC resource file which was provided by the software vendor. It was later discovered that the AGC resource file contained a software switch which automatically switched from TLB to CF upon loss of Tie Line telemetry. Tie Line telemetry loss did occur due to a momentary loss of telecommunications at a single site. Throughout the period (from the time of the automatic switch until software support personnel identified cause of inappropriate Area Control Error (ACE) calculation), the AGC calculated ACE did not compare Net Actual and Net Scheduled Interchange. The AGC resource file was promptly corrected upon discovery of the error at 05:58 a.m. EST.	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 improper operational mode of the entity's AGC could not have resulted in undue deviation in the system frequency. Also the system frequency component of ACE was being continuously monitored by the entity's Energy Management System (EMS) system operators.	Mitigation included correcting deficiencies in its cyber security change control program to address peer review of application control file changes and further, the entity updated the display of ACE and ACE control process when involving AGC switching. AGC alarms and locations of alarms for SCADA displays for the operators were also included. The entity completed mitigation as verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900268	EOP-001-0	R6	The entity was found during a compliance audit that it did not provide its emergency generating capacity shortage plan, its system restoration plan, and its firm load shed plan to its Reliability Coordinator (RC) and neighboring Transmission Operators (TOPs) and Balancing Authorities (BAs) for a 16-month period. Also, the entity did not provide its response to the transmission limit violations plan and its contingencies plan to its RC and neighboring TOPs and BAs for a 19-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was able to demonstrate it had restoration plans in place and could have provided them upon request. Further, the entity had provided sufficient training to its staff to execute the restoration plans correctly when such a need arises.	Mitigation included submitting the plans to the FRCC secure website where it is available to its RC and neighboring TOPs and BAs. Further, the plans were sent by registered mail for acknowledgment of shared plans to the RC and neighboring TOPs and BAs. Mitigation was completed and verified by FRCC.

Attachment A-1

October 31, 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 10 (FRCC_URE10)	NCRXXXXX	FRCC200900270	EOP-005-1	R4	The entity was found during a compliance audit that it did not coordinate its restoration plans with its Reliability Coordinator (RC) and neighboring TOPs and Balancing Authorities (BAs) for a 16-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was able to demonstrate it had restoration plans in place and could have provided them upon request. Further, the entity had provided sufficient training to its staff to execute the restoration plans correctly when such a need arises.	Mitigation included submitting the plans to the FRCC secure website where it is available to its RC and neighboring TOPs and BAs. Further, the plans were sent by registered mail for acknowledgment of shared plans to the RC and neighboring TOPs and BAs. Mitigation was completed and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900272	PER-002-0	R1	The entity during a compliance audit was unable to demonstrate it trained its operating personnel and was staffed with adequately trained operating personnel for a 31-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity's operating personnel were NERC certified operators, they met the annual required 32 hours of emergency operations training, and the entity trained all of its personnel in its system restoration procedures. Due to entity limited staff availability and the detailed training guidelines set forth by the training program, some personnel were not able to complete a few of the required topics. Two out of nine system operators did not complete a few of the required topics. All the system operators maintained their certification and completed the required training for maintaining certified system operator credentials.	The entity completed all the milestones to address lack of system operator training and compliance documentation maintenance. The entity training included training on principles of BPS operation, emergency plans, and NERC standards and practices. Further, the entity hired system operations training personnel and added training resources for system operator training. Mitigation was completed and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900273	PER-002-0	R3; R3.4	The entity during a compliance audit was unable to demonstrate that its training staff was identified for a 19-month period. Also, the evidence was insufficient to demonstrate that its entire training staff identified in the training program document was competent in both knowledge of system operations and instructional capabilities for a one-year period (R3.4).	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 was able to demonstrate that it was training its operating personnel using subject matter experts and training by committee throughout the duration of the remediated issue. Evidence was sufficient to demonstrate that one individual out of four was competent in both knowledge of system operations and instructional capabilities. The other three individuals were competent in knowledge of system operations but lacked credentials to demonstrate their instructional capability.	The entity completed all the milestones to address lack of system operator training and compliance documentation maintenance. The entity training included training on principles of BPS operation, emergency plans, and NERC standards and practices. Further, the entity hired system operations training personnel and added training resources for system operator training. Mitigation was completed and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC200900274	PER-002-0	R4	The entity during a compliance audit was unable to demonstrate that it provided its operating personnel the other training, as identified in the requirement, required to maintain qualified operating personnel for two years.	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's operating personnel were NERC certified operators, they met the annual required 32 hours of emergency operations training, and the entity trained all of its personnel in its system restoration procedures. Due to entity limited staff availability and the detailed training guidelines set forth by the training program, some personnel were not able to complete a few of the other required topics. 2 out of 9 system operators did not complete a few of the required topics. All the system operators maintained their certification and completed the required training for maintaining certified system operator credentials.	The entity completed all the milestones to address lack of system operator training and compliance documentation maintenance. The entity training included training on principles of BPS operation, emergency plans, and NERC standards and practices. Further, the entity hired system operations training personnel and added training resources for system operator training. Mitigation was completed and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC201100414	INT-006-3	R1	The entity self-reported that it did not respond to 12 On-time Requests for Interchange (RFIs) within the required time period for a two-month period.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: the delay of approval of the tags, by typically just a few minutes, resulted in economic only impact to only 12 RFI transactions no greater than 100 MW.	The entity developed a formal system operation practice for identifying the responsibilities and actions required associated with RFIs. Further, the entity included training modules and steps for increasing operator awareness and imparting face to face review of the updated procedures. Mitigation was completed by the entity and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC201000305	CIP-004-1	R3	The entity self-reported that one of its employees who was granted access to Critical Cyber Assets (CCAs) did not undergo a personnel risk assessment (PRA) within 30 days of being granted such access as required by CIP-004 R3. The required PRA was completed 43 days after the required date.	This issue posed a minimal risk and did not pose serious or substantial risk to the reliability of the BPS because the employee whose PRA was delayed was a longtime employee who already had access to the CCAs. The employee underwent a PRA within 73 days instead of 30, with satisfactory results. Since the employee already had access, delay in undergoing a PRA did not increase any potential risk to the BPS reliability. CIP-004-1 R3 allowed 30 days for conducting a PRA. The additional 43 days would not have added significant risk for an employee of long term standing who has been with the organization for 8 years.	Mitigation milestones included completion of pending PRA for one person, training for all concerned personnel who are involved in granting access to the Physical Security Perimeter (PSP) and revision of procedures for granting unescorted physical access to the PSP. Further, the entity modified technical controls in the physical access control systems to ensure that PRA and training dates are entered for verification prior to granting authorized physical access to the PSP. Mitigation was completed by the entity and verified by FRCC.

Attachment A-1

October 31, 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 10 (FRCC_URE10)	NCRXXXXX	FRCC201000361	CIP-004-1	R2.1	The entity self-reported that one of its employees was not trained prior to being granted physical and logical access to the entity's Critical Cyber Assets (CCAs).	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 training was delayed by five days only and the concerned person was in the control room environment and was being trained under constant supervision of his/her peers. During the initial training the identified person did not operate the CCA (BPS control) independently without supervision. All his/her activities were supervised and under the guidance of experienced peers who were training under the CIP program.	Mitigation milestones included completion of pending training for one person and revision of procedures for granting authorized access to the CCA and to include exact code of the required training modules to limit any confusion with completion of other NERC and FERC related training which was recognized as the original root cause of the remediated issue. Mitigation was completed by the entity and verified by FRCC.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 10 (FRCC_URE10)	NCRXXXXX	FRCC201100426	CIP-004-3	R4.1	The entity self-reported that it did not update the list of all authorized users with electronic or unescorted physical access within seven days from date of change as required by CIP-004 R4.1. One duplicate entry for a person who had retired was erroneously left on the list because the concerned person was listed twice on the list with one entry stating that access had been disabled. The record with correct access status was removed during the seven day update window, but the other entry was not removed due to oversight. The error was recognized during a quarterly review 50 days after the required date and the list was corrected immediately.	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 access cards were physically destroyed and access was revoked timely but only the list was not updated. The identified person could not have gained access without completing the complete process for gaining authorized access with an access card, which would involve a control check by a supervisor and the Critical Cyber Asset access control department.	Mitigation included steps to review all user profile on the list and remove any duplicate entries. Further, the entity modified the procedure to ensure that any new access or lost card badge requests are treated as new user access request and all controls and verification are applied. Mitigation also included further training of the staff involved with the verification and access provisioning process. The identified person's duplicate entry was removed from the list. Mitigation was completed by the entity and verified by FRCC.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201000242	CIP-007-2	R5.1.1; R5.1.2	The entity self-reported noncompliance with CIP-007-2 R5 because it failed to ensure that user accounts were implemented as required by R5.1.1, and did not maintain logs for 90 days as required by R5.1.2. During a quarterly personnel access review, the entity discovered that access for one individual (<1%) was granted without documented authorization in accordance with CIP-007 R5.1. One of the entity's administrators discovered that during that quarter, operator system level user activity logs had not been capturing failed authentication attempts. Since successful authentications were still being captured, more than 90 calendar days of logs were available for review. The issue was resolved on the same day it was discovered and failed authentication attempts were captured again. The total number of days for which failed authentication was not logged was 40 calendar days.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had the following protective measures in place: (1) system access configuration logs were verified for the duration of the lapse and no suspicious account setups were present; (2) the number of accounts with logon rights to the servers is limited; (3) group policy object limits the number of failed logons before the account is locked; (4) firewall rules and ports are locked to only allow necessary communication; (5) the anti-virus monitors and corrects malicious events on the servers; (6) the intrusion detection system monitors and corrects malicious events on the network; (7) a system manager monitors server connectivity to network and detects and reports any changes to the hardware on the server; and (8) the entity's physical security limits physical access to the servers.	The entity performed the following actions to mitigate the remediated issue: (1) added servers back to program which limits number of failed logons before account is locked out; (2) fixed the script; and (3) tested to ensure logs were sent, received, and that monitoring and alerting functionality were operational. Mitigation has been completed and verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE2)	NCRXXXXX	MRO201000244	CIP-007-1	R5.1.1	The entity self-reported noncompliance with CIP-007-1 R5.1.1 because it failed to ensure that user accounts were implemented as approved by designated personnel. A cyber access account was created and access was allowed to critical facilities for 59 days without documented approval and authorization as required in CIP-007-1 R5.1.1. The entity reported that this issue occurred because an individual failed to follow the corporate procedure for CIP access when transferring from one job function to another within the entity.	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 access was appropriate for the affected individual and the access remained configured in the servers. Additionally, the steward gave verbal approval, and the individual had personnel risk assessment (PRA) and cyber security training as required by CIP-004-1 R2 and R3.	The entity performed the following actions to mitigate the remediated issue: (1) verified that NERC CIP training and PRA prerequisites were met; and (2) ensured that subject matter experts understood the requirements for formal, documented approval of NERC CIP cyber access. Mitigation has been completed and verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE3)	NCRXXXXX	MRO201000235	PRC-004-1	R3	During a regularly scheduled compliance audit, MRO determined that the entity and its member entity failed to provide MRO documentation of its Misoperations analyses and Corrective Action Plan for the Protection System Misoperation of a relay which experienced a Misoperation on August 29, 2009.	The remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although the member entity failed to submit its Misoperations analysis and Corrective Action Plan, the member entity did perform the analysis and implemented a Corrective Action Plan.	On behalf of its member entity, the entity submitted the Misoperation analyses and Corrective Action Plan report for the relay Misoperation to MRO. This submittal included a revised quarterly MRO Misoperation report. Mitigation has been completed and verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100296	CIP-004-1	R4	The entity self-reported noncompliance with CIP-004-1 R4 because it failed to review a Critical Cyber Asset (CCA) access list during the first quarter in which the entity was required to comply under the CIP Implementation Table. The CCA access list was reviewed starting in the next quarter.	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 only one CCA access list was not reviewed for one quarter. Additionally, upon review, the entity did not identify any individuals that had access during that time that should have been removed from the list.	This remediated issue was mitigated when the entity reviewed the CCA access list for the second quarter of 2010.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100299	CIP-005-1	R3	The entity self-reported noncompliance with CIP-005-1 R3 because it did not have a monitoring process documented or implemented for one category of Critical Cyber Asset (CCA) access devices. Logs were generated as of the date the entity was required to comply with the Standard under the CIP Implementation Table; however, they were not being monitored until three months later. The security review and logging procedures for these devices were formally documented and published six months after the compliance date.	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 individuals with access to the devices were properly authorized, trained and had current personnel risk assessments. The deficiency was in the maintenance of the activity log for the category of devices for slightly longer than 90 days; however, authentication methods existed during the time of the issue.	The security review and logging procedures for the CCA devices were formally documented and published.

Attachment A-1

October 31, 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
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100305	CIP-007-1	R5	The entity self-reported noncompliance with CIP-007-1 R5 because it failed to have an audit trail of the shared account use. Specifically, the audit trails of the account use of shared accounts on the transmission management system (TMS), and two accounts in the substation network were not maintained as of the date of mandatory compliance, for one month for the TMS accounts and for three months for the substation accounts.	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 individuals with access to the shared accounts were properly authorized, trained and had current personnel risk assessments. The deficiency was in the maintenance of the activity log and no incidents occurred during the period of deficiency.	The entity now maintains audit trails for shared account use for all required accounts.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 4 (MRO_URE4)	NCRXXXXX	MRO201100306	CIP-007-1	R6	The entity self-reported noncompliance with CIP-007-1 R6.5 because it failed to document reviewing logs for all system events for Cyber Assets within the Electronic Security Perimeter (ESP). Specifically, the entity failed to review the security logs from the transmission management system (TMS) for a two month period. The security logs for these systems existed but they were not reviewed.	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 at all times, including this period of time, the entity was continuing to monitor all Cyber Assets with the ESP for security events. Automated and manual alerts were available to be issued on the detection of any such event. Subsequent review of those logs revealed there were no threatening anomalies during the period of time in question.	The entity completed review of its security logs and implemented procedures to ensure regular security log review.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5)	NCRXXXXX	MRO201000204	PRC-008-0	R2	During a regularly scheduled compliance audit, MRO randomly selected Under Frequency Load Shedding (UFLS) devices and requested maintenance and testing records for the equipment associated with those circuits. Upon request, the entity reported that it was missing evidence of maintenance and testing records for several of the devices. MRO then requested that the entity perform a full inventory of its maintenance and testing records for all of its Protection System devices subject to PRC-008-0 R2. In response, the entity reported that it has 169 devices subject to PRC-008-0 R2, including 33 UFLS relays, 79 voltage and current sensing devices, 24 station batteries and 33 DC control circuits. Of the 169 devices, the entity failed to provide evidence for 5 UFLS station batteries, or approximately 3% of the devices.	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's total loads that would be affected by the 5 UFLS station batteries devices are 17% of the total UFLS load shed for which the entity is responsible. Additionally, the entity continuously monitors DC power supply to the UFLS devices on SCADA, and upon retesting the equipment, the entity did not identify any issues with UFLS devices. Tests indicated no damage or out of tolerance settings for any of its UFLS devices.	The entity performed the following to mitigate the remediated issue: (1) a comprehensive review of the UFLS equipment for all substations subject to PRC-008; (2) all maintenance and testing of equipment lacking maintenance and testing records; (3) sent a letter to the personnel responsible for the maintenance and testing of the entity's Protection Systems along with its current transmission and generation Protection System maintenance and testing program (Program) and required individual acknowledgments by those personnel stating that they have read the Program and will perform their related tasks required by the Program in a timely manner; and (4) sent a written assignment to the electric transmission department at the entity's general office instructing them to keep track of the tasks required by the Program, maintain a database for the completion dates, and coordinate these tasks with all involved personnel. Mitigation has been completed and verified by MRO.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 5 (MRO_URE5)	NCRXXXXX	MRO201100370	CIP-004-3	R4; R4.2	The entity self-reported noncompliance with CIP-004-3 R4.2 because it failed to update its Critical Cyber Assets (CCAs) access list for a contractor within 7 days from when the contractor no longer required access. The entity's janitorial service company notified the entity building and grounds supervisor late in the day that one of its employees assigned to clean within the Physical Security Perimeter (PSP) was no longer employed with the janitorial services company as of that date. The building and grounds supervisor notified the entity system operator on duty, and left a telephone voice message for the entity electric compliance manager regarding this change at 4:46 p.m. CST; however, the electric compliance manager was on vacation, and the telephone voice message was not attended. The building and grounds supervisor also immediately revoked building access for the employee at that time. Additionally, the system operator on duty made note of this change in the logbook, kept within the control room, which lists the janitorial service employees that are allowed access to the PSP. At no time did the terminated janitorial service employee have physical access to the entity general office building or the control room. The electric compliance manager returned from vacation ten days later, and learned of the change at that time.	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 deficiency related to updating the access list was promptly corrected and the actual physical access had been revoked. Access to the general office building is needed before any attempt could be made to request or gain access to the defined PSP.	The entity performed the following actions to mitigate the remediated issue: (1) revoked limited unescorted physical access and will no longer consider contractor personnel as having limited physical access to certain areas within the designated PSP. They are now considered escorted visitors whenever they are within the PSP; (2) because contractors no longer have limited physical access to certain areas within the designated security perimeter, these specific people were removed from the entity's CCAs access list; (3) for additional security, the entity installed a keyed lock on a side door within the control room restroom that could possibly be used to access an area within the PSP that contains CCAs. This door will remain locked, and only be unlocked when the door is needed by personnel having unescorted physical or logical access to the entity's CCAs; (4) installed an alarm on the door, that when opened, generates an Energy Management System (EMS) alarm to alert the system operator; and (5) when notified of any changes in contractor personnel, the entity building and grounds personnel have been instructed to make actual voice contact with either the entity NERC compliance analyst, electric compliance manager, or the manager of electric system operations and planning. These people are responsible for maintaining the CCAs access list, along with access to the logical or PSP. Mitigation has been completed and verified by MRO.

Attachment A-1

October 31, 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
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100239	CIP-003-1	R1; R1.3	During an NPCC CIP compliance audit it was found that the entity was in noncompliance with CIP-003-1 R1. NPCC determined that the entity had a NERC cyber security policy and statement of management commitment not signed by the senior manager assigned pursuant to CIP-003 R2.	The remediated issue posed a minimal risk to the reliability of the bulk power system because although the policy was not signed by the senior manager assigned pursuant to CIP-003 R2, the policy was reviewed by the digital risk and security group, who performs annual review covering all NERC CIP-related information security requirements, and signed by the chief information security officer. The chief information security officer was designated by the senior manager as his/her delegate pursuant of CIP-003 R2.3.	The entity reviewed and received approval of the cyber security policy by the senior manager assigned pursuant to CIP-003 R2. The entity completed its mitigation activity as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100240	CIP-007-2a	R9	During a NPCC CIP compliance audit it was found that, the entity was in noncompliance with CIP-007-2a R9. NPCC determined that the entity's parent company's information security standard testing document was not corrected to change its 90-day requirement to a 30-day requirement as required by the change in CIP-007-2a R9; however, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3.	The remediated issue posed a minimal risk to the reliability of the bulk power system because there were no Cyber Security Incidents that required action pursuant to the Cyber Security Incident response plan during the 8-month period until the plan was updated to reflect the 30-day update period in accordance with CIP-007-2. In addition, the annual procedure review was performed in conformity with the Standard and updated to reflect the changes reflected in CIP-007-3	The entity's parent company's information security standard testing document was updated, changing the ninety calendar day update requirement to the thirty calendar day update requirement. The entity completed its mitigation activity as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100241	CIP-008-2	R1; R1.4	During a NPCC CIP compliance audit it was found that the entity was in noncompliance with CIP-008-2 R1. NPCC determined that the entity's parent company's information security standard incident management document was approved to require a process for updating the Cyber Security Incident response plan within 30 days of any changes as per CIP-008-3 R1.4. This was done 70 days after its obligation to meet the 30-day requirement.	The remediated issue posed a minimal risk to the reliability of the bulk power system because the information security standard incident management document was updated within a short period of time - only 2 months after the 30-day criteria went into effect, changing the ninety calendar day update requirement to the thirty calendar day update requirement. No interim and future risks were identified.	The entity's parent company's information security standard incident management document was approved with the update to require a process for updating the Cyber Security Incident response plan within 30 days of any changes as per CIP-008 R1.4 prior to the CIP audit. No further action to mitigate this violation was necessary. The entity completed its mitigation activity as verified by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100243	CIP-009-1	R4	During a NPCC CIP compliance audit it was found that the entity was in noncompliance with CIP-009-1 R4. NPCC determined that there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storage of information required to successfully restore Critical Cyber Assets (CCAs).	The remediated issue posed a minimal risk to the reliability of the bulk power system because evidence was provided that although there was no documentation in the entity's disaster recovery procedures that addressed a process for backing up and storage of information required to successfully restore CCAs, the backup and storage of information required to successfully restore CCAs was taking place.	The entity revised its disaster recovery procedures to include references to its change control and configuration procedure. The entity also revised this change control and configuration procedure to address CIP-009 R4 backup and restore requirements. The entity completed its mitigation activity as verified by NPCC.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC200900297	CIP-004-1	R2; R2.1	During a Spot Check Reliability*First* identified an issue concerning CIP-004-1 R2.1. The entity failed to address in its training program, in effect from July 1, 2008 to July 5, 2009, the proper use of Critical Cyber Assets (CCAs) as required by CIP-004-1 R2.2.1, or the action plans and procedures to recover CCAs following a Cyber Security Incident, as required by CIP-004-1 R2.2.4.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). The risk to the BPS was mitigated by the fact that although the prior training program did not directly address the proper use of CCAs or action plans and procedures to recover CCAs following a Cyber Security Incident, it contained references to the entity policies and procedures that govern the proper use of CCAs and action plans and procedures to recover CCAs following a Cyber Security Incident.	The entity revised its cyber security training program to include training material about the proper use of CCAs and to include action plans and procedures to recover or re-establish CCAs and access thereto following a Cyber Security Incident. The entity mitigated the issue as verified by Reliability*First*.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201000436	CIP-003-1	R4	The entity submitted a Self-Report to Reliability*First* indicating an issue with CIP-003-1 R4. The entity has a documented information protection program to identify, classify, and protect information associated with Critical Cyber Assets (CCAs). This program requires that the entity encrypt all information associated with CCAs before digitally transferring that information outside of the company. The entity, contrary to this program, submitted an unencrypted Technical Feasibility Exception (TFE) request, which included information associated with a CCA, to Reliability*First*.	In light of the nature of the issue, offset by the mitigating factors, ReliabilityFirst determined that this issue posed a minimal risk to the reliability of the bulk power system (BPS). At the time of the incident, the entity verbally confirmed that Reliability*First* received the unencrypted transmission. Reliability*First* was the only external addressee on the email and, to the entity's knowledge the only external recipient of the unencrypted email. Moreover, the entity has confirmed that the entity's internal email system is protected by controls which effectively prevent unauthorized access to the email in question. The entity also claims that only authorized individuals have had access to the email in question.	The entity trained two employees to be responsible for externally transmitting all CCA related information via encryption. The entity has implemented a technical control to quarantine messages labeled for encryption. The entity will also develop and distribute awareness materials to stress conformity with procedures to use email encryption prior to electronically transmitting information concerning CCAs. Pursuant to an extension requested by the entity, and a subsequent approval of that request granted by Reliability*First*, the entity completed mitigation.

Attachment A-1

October 31, 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 2 (RFC_URE2)	NCRXXXXX	RFC201000458	CIP-003-1	R1	The entity submitted a Self-Report identifying an issue with CIP-003-1 R1. Due to security software incompatibility, the entity could not access certain Critical Cyber Assets (CCAs) to change passwords every 60 days as required by the entity's cyber security policy. The entity drafted its cyber security policy to comply with Reliability Standard CIP-007 R5. The entity's policy to change passwords every 60 days is more stringent than CIP-007 R5, which requires an entity change its password "at least annually or more frequently based on risk." Under the entity's cyber security policy the entity should have changed the user account passwords on its identified CCAs but did not do so until approximately six months after the expected date.	Reliability*First* found that the issue posed a minimal risk to the reliability of the bulk power system (BPS) as the entity was adhering to the password requirements pursuant to CIP-007 R5, but had established a more stringent 60 day time frame for changing passwords associated with CCAs. The entity's more stringent 60-day password change requirement was not established to address any heightened risk, but rather to ensure consistency with a general corporate information assurance practice of changing all IT system passwords every 60 days. Accordingly, the entity's failure to act in strict accordance with the 60 day password policy does not represent a failure to address any known potential cyber risk. Moreover, the security software incompatibility that contributed to the entity's password change delay within its internal 60-day timeframe effectively prevented anyone from gaining access to the identified CCAs for those six months. The entity has confirmed that there was no access to the identified CCAs during this time period. Furthermore, the entity has also confirmed that there were no personnel changes during the time period in question involving those individuals authorized to access these CCAs.	The entity installed a separate terminal within the entity's Electronic Security Perimeter. This terminal gave the entity man-to-machine access to the identified CCAs and thus allowed it to change all user account passwords on the them. Pursuant to an extension requested by the entity and a subsequent approval of that request granted by Reliability*First*, the entity completed mitigation.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000667	EOP-004-1	R3; R3.1	The entity submitted a Self-Report to Reliability*First* identifying a possible issue with EOP-004-1 R3.1. The entity experienced a storm that resulted in loss of power to more than 50,000 customers for more than one hour. The entity submitted the preliminary written report submitted to the U.S. Department of Energy (Preliminary Report) of the storm to Reliability*First* and NERC approximately seven months after the required 24-hour reporting period.	In light of the nature of the issue, offset by the mitigating factors, Reliability*First* determined that the issue posed a minimal 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 reportable incident was storm-related, and the entity submitted the Preliminary Report to the Department of Energy (DOE) within 48 hours for the reportable incident.	The entity conducted training on its revised emergency procedures to promote awareness and reinforce the importance of EOP-004-1 to its employees. In addition, the entity revised its emergency notification procedures by identifying the responsible staff for submitting the Preliminary Report, adding DOE notification instructions, and clarifying the appropriate process for submission of the Preliminary Report and final DOE Report. The entity notified the relevant personnel of these revisions. Upon identifying the full extent of the issue, the entity developed a matrix for emergency notification procedures to assist personnel in quickly identifying appropriate responsibilities and tasks, and further revised and disseminated its emergency notification procedures to reflect these revisions. The entity completed mitigation activities for the issue.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000411	CIP-005-1	R2; R2.6	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted one late TFE Request for CIP-005-1 R2.6.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that the entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as using two-factor authentication and firewall rules that minimize exposure of devices. Many of these compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of its system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]." Moreover, after the submission of the TFE Requests, the entity also identified and implemented additional measures, which exceeded the required compensating measures and further reduced any potential risk. For example, the entity identified a vendor solution that provides a method of implementing acceptable use banners.	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.

Attachment A-1

October 31, 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	RFC201000412	CIP-007-1	R3	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted three late TFE Requests for CIP-007-1 R3.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as performing vulnerability scans on the network and monitoring network traffic. Many of the compensating measures were in place well before the effective date of the CIP Standards. The systems also reside within a Physical Security Perimeter and an Electronic Security Perimeter. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of its system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000413	CIP-007-1	R4	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted three late TFE Requests for CIP-007-1 R4.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as preventing the system from connecting to the internet through firewall restrictions and preventing users from directly installing software on the system. Many of these compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000414	CIP-007-1	R5	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted nine late TFE Requests for CIP-007-1 R5.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as requiring frequent password changes through policies and procedural requirements for password length and complexity. The entity also monitors and tracks system log files for unusual user activity, performs background checks on all users, and users connect through a network protocol for secure remote login and other secure network services over an insecure network, which encrypts passwords. Many of the compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.

Attachment A-1

October 31, 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 4 (RFC_URE4)	NCRXXXXX	RFC201000415	CIP-005-1	R2; R2.6	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted one late TFE Request for CIP-005-1 R2.6.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as using two-factor authentication and firewall rules that minimize exposure of devices. Many of these compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]." Moreover, the entity also identified and implemented additional measures after the submission of the TFE Requests, which exceed the required compensating measures and further reduced any potential risk. For example, the entity identified a vendor solution that provides a method of implementing acceptable use banners.	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201000417	CIP-007-1	R3	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted two late TFE Request for CIP-007-1 R3.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as performing vulnerability scans on the network and monitoring network traffic. The systems also reside within a Physical Security Perimeter and an Electronic Security Perimeter. Many of these compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201100418	CIP-007-1	R4	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted three late TFE Requests for CIP-007-1 R4.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as preventing the system from connecting to the internet through firewall restrictions and preventing users from directly installing software on the system. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.

Attachment A-1

October 31, 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 4 (RFC_URE4)	NCRXXXXX	RFC201000419	CIP-007-1	R5	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted 11 late TFE Requests for CIP-007-1 R5.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as requiring frequent password changes through policies and procedural requirements for password length and complexity. The entity also monitors and tracks system log files for unusual user activity, performs background checks on all users, and users connect through a network protocol for secure remote login and other secure network services over an insecure network, which encrypts passwords. Many of these compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000420	CIP-005-1	R2; R2.6	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically-the entity-submitted one late TFE Request for CIP-005-1 R2.6.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that the entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as using two-factor authentication and firewall rules that minimize exposure of devices. Many of the compensating measures were in place well before the effective date of the CIP Standards. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of its system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]." Moreover, after the submission of the TFE Requests, the entity also identified and implemented additional measures which exceeded the required compensating measures and further reduced any potential risk. For example, the entity identified a vendor solution that provides a method of implementing acceptable use banners.	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000421	CIP-007-1	R3	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted one late TFE Request for CIP-007-1 R3.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place such as performing vulnerability scans on the network and monitoring network traffic. Many of these compensating measures were in place well before the effective date of the CIP Standards. The systems also reside within a Physical Security Perimeter and an Electronic Security Perimeter. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of its system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.

Attachment A-1

October 31, 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 5 (RFC_URE5)	NCRXXXXX	RFC201000422	CIP-007-1	R4	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted four late TFE Requests for CIP-007-1 R4.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as preventing the system from connecting to the internet through firewall restrictions and preventing users from directly installing software on the system. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000423	CIP-007-1	R5	The entity self-reported an issue with the CIP Standards arising from the entity's failure to timely submit Technical Feasibility Exception (TFE) Requests in accordance with NERC procedures. The Self-Reports referenced all identified TFEs that should have been filed as of that point. The entity subsequently conducted an extent-of-condition investigation and identified four additional needed TFEs. The TFE Requests for the entity were submitted between approximately five and fifteen months late. Specifically, the entity submitted 18 late TFE Requests for CIP-007-1 R5.	Reliability*First* 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 formal TFE Requests. Reliability*First* determined that entity's system is structured with many firewall and other security controls. As of the effective date of the CIP Standards, there were compensating measures in place, such as requiring frequent password changes through policies and procedural requirements for password length and complexity. The entity also monitors and tracks system log files for unusual user activity, performs background checks on all users, and users connect through a network protocol for secure remote login and other secure network services over an insecure network, which encrypts passwords. Therefore, although the entity submitted untimely TFE Requests, the entity was performing compensating measures to ensure the basic security of the entity's system throughout the duration of the issue. Reliability*First* accepted and approved the TFE Requests' compensating measures because they "achieve at least a comparable level of security for the Bulk Electric System as would Strict Compliance with the [CIP Standards]."	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.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 1 (SERC_URE1) Southwest Louisiana Electric Membership Corporation (SLEMCO)	NCRXXXXX	SERC2011007287	CIP-003-2	R2	During an Off-Site Audit conducted by SERC, SERC_URE1 failed to provide evidence that a single senior manager had been assigned with overall responsibility and authority for CIP-002 through CIP-009, as required. SERC_URE1 designated overall responsibility and authority to a senior manager on April 4, 2011, and identified the senior manager by name, title, and date of designation.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. SERC_URE1 has no Critical Assets. 2. SERC_URE1 does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4.	SERC_URE1 completed the following action: Assigned a senior manager with the overall responsibility and authority for leading and managing the implementation of and adherence to CIP-002 through CIP-009 on April 4, 2011. SERC staff verified completion of the mitigation activity.
SERC Reliability Corporation (SERC)	Unidentified Registered Entity 2 (SERC_URE2)	NCRXXXXX	SERC201000530	IRO-004-1	R4	SERC_URE2 submitted a Self-Report to SERC stating that it had failed to provide any of the information required by IRO-004-1 R4 to its Reliability Coordinator (RC) for approximately seven months.	SERC determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The generator at issue is not an available resource to the RC since it is dedicated to SERC_URE2's native load. 2. SERC_URE2 is primarily a cogeneration operation with no critical facilities. 3. SERC_URE2's gross and net load rolling forecasts are provided to the LSE's emergency management organization 24 hours a day, seven days a week. 4. SERC_URE2 has no operating reserves. 5. SERC_URE2 has no interchange transaction.	SERC_URE2 completed the following action: A communications protocol was developed to directly provide the required information to the RC. SERC staff verified completion of the mitigation activity.

Attachment A-1

October 31, 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_URE1)	NCRXXXXX	SPP201000232	CIP-004-1	R3; R3.1; R3.3	SPP_URE1 submitted a Self-Report to the SPP RE stating that it had an issue with this Reliability Standard. Upon further investigation of the facts and circumstances, including a subsequent Spot Check, SPP RE determined that SPP_URE1 was noncompliant with CIP-004-1 R3.1 and R3.3. CIP-004-1 R3.1 During an internal compliance assessment, SPP_URE1 discovered that although it documented and implemented its Personnel Risk Assessment (PRA) program by the date the Standard became effective (July 1, 2008), PRAs for current employees that were conducted prior to the effective date of the Standard were based on a five-year criminal background rather than a seven-year time interval and as a result SPP_URE1 failed to conduct the PRAs within the seven-year timeframe after the Standard became effective. All new PRAs conducted after the effective date of the Standard were based on a seven-year time period. CIP-004-1 R3.3 SPP_URE1 also discovered, during its internal assessment, that it was unable to locate PRAs for six individuals with unescorted physical access to CCAs. These individuals gained authorized access on July 1, 2008. On January 13, 2010, background checks with a seven-year time interval were requested on all six individuals, and the PRAs were completed on January 27, 2010. During a Spot Check, SPP RE discovered an additional instance where a SPP_URE1 security integrator contractor with unescorted physical access rights did not have a PRA. The contractor was previously given access in July 2008 to unrestricted areas within SPP_URE1's main office. Therefore, a PRA was neither required nor conducted. However, on July 1, 2008, SPP_URE1 expanded its physical security perimeter (PSP) to include a stairwell door that leads to a secured access door to its Control Center but failed to remove the contractor's access rights to the stairwell door until August 27, 2008, the date the oversight was discovered. The access logs show that the contractor never used his credentials to access the stairwell door.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although the background checks did not strictly adhere to the Standard, they were conducted, and the five-year interval covered a significant portion of the required seven-year time period. Additionally, regarding the six individuals in which no PRAs could be located, all were long-term trusted employees with no disciplinary actions who had received the required cyber security training. With respect to the contractor who was inadvertently granted access to a newly identified restricted area without a PRA, the oversight was discovered and corrected less than two months (58 days) after access was granted, and the contractor never attempted to use his credentials to enter the PSP. Even if the contractor had used his credentials to open the stairwell door, his credentials would not have allowed him to open the secured door to the control center. Additionally, after PRAs had been conducted on the six individuals having authorized cyber or authorized unescorted physical access to CCAs, no PRA came back as having failed.	SPP_URE1 revised its PRA procedures to clarify the roles for personnel responsible for implementing its PRA program. Additionally, on January 13, 2010, SPP_URE1 requested new PRAs with seven-year background checks for the six individuals whom PRAs could not be located, which were completed on January 27, 2010. SPP_URE1 also conducted new PRAs for all remaining personnel having authorized cyber or authorized unescorted physical access to CCAs. All PRAs were completed on March 30, 2010. Regarding the contractor with inadvertent unescorted physical access to an access point to SPP_URE1's PSP, SPP_URE1 revoked such access on August 27, 2008. SPP_URE1 revised its PSP to require all changes that may impact physical security measure to first be sent in writing to a security manager prior to changes being made. This allows preplanning and discovery of any potential logging or monitoring changes that will need to be addressed after approval of such changes. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCRXXXXX	SPP201000293	CIP-006-1	R1.8	SPP_URE1 self-reported an issue with this Standard. Specifically, during an internal compliance assessment, SPP_URE1 discovered that it was unable to locate personnel risk assessments (PRAs) for five SPP_URE1 IT technicians and one SPP_URE1 security contractor who had access to one of its servers, which is a Cyber Asset (CA) used to control and monitor access of SPP_URE1's physical security perimeters (PSPs). These individuals gained authorized access on July 1, 2008. Background checks were requested for all individuals and completed PRAs were received on April 14, 2010.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. The five IT technicians were long-term trusted employees with no disciplinary actions who had received the required cyber security training. Additionally, the contractor was a trusted vendor, who had been vetted for his employment. Additionally, after PRAs had been conducted on these six individuals, no PRA came back as having failed.	PRAs were completed as of April 14, 2010. To prevent reoccurrence of this issue, SPP_URE1 revised its Cyber Security Policy to restrict physical access to the server to only those with a business need. The policy now requires physical access to the server be requested and approved through SPP_URE1's facilities access request process, which incorporates the management authorization of the access, training prerequisites, or PRAs needed in order to be granted access. SPP_URE1 implemented additional security measures to its server room to further secure the server. For instance, SPP_URE1 installed a server rack with secured doors that can only be opened by a newly installed card reader that is attached to the rack. Moreover, unauthorized attempts to the server will now sound an alarm to SPP_URE1 personnel who remain located inside the facility where the server room is located 24 hours a day, 7 days a week. Access to the server remains monitored by security personnel 24 hours a day, 7 days a week with a camera that is installed in the server room. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.

Attachment A-1

October 31, 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_URE1)	NCRXXXXX	SPP201000325	CIP-002-1	R3	During a spot check, SPP RE determined that SPP_URE1 was noncompliant with CIP-002-1 R3 for incorrectly identifying ten network switches located within SPP_URE1's Electronic Security Perimeter (ESP). Specifically, the switches were identified as Protected Cyber Assets (PCAs) but they should have been identified as CCAs because they are the communication interface between the operator consoles and the some of SPP_URE1's systems and essential to the reliable operation of SPP_URE1's control center.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). In SPP_URE1's cyber environment, PCAs and CCAs are afforded the same cyber security protection measures. Therefore, although the network switches were incorrectly identified, in practice, the switches were treated as CCAs. Consequently, the misclassification of the network switches had no actual impact to the reliability of the BPS, and there was no increased risk to the reliability of the BPS.	SPP_URE1 applied its Control Center CCA process to the network switches, changed the identification of the switches from PCAs to CCAs, and updated its CCA identification list to reflect the change. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCRXXXXX	SPP201000326	CIP-003-1	R1; R1.1; R1.2	During a spot check, SPP RE determined that SPP_URE1 was noncompliant with CIP-003-1 R1.1 and R1.2. Regarding R1.1, SPP_URE1's 2008 version of its Cyber Security Policy did not include any provisions for emergency situations. This issue was remediated in a subsequent version of the policy, which became effective on June 30, 2009. Regarding R1.2, SPP_URE1 was unable to demonstrate that it provided the Cyber Security Policy to its vendor personnel who had access to, or was responsible for, CCAs prior to April 13, 2010.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Regarding R1.1, although SPP_URE1 failed to include provisions for emergency situations in its 2008 version of its Cyber Security Policy, it did have a robust Cyber Security Policy demonstrating management's commitment to implementing a program for compliance with the CIP Standards. Additionally, its 2009 version of the Cyber Security Policy provided provisions for emergency situations. Regarding R1.2, the Cyber Security Policy was uploaded on SPP_URE1's intranet and made available to SPP_URE1's systems vendor upon request. While the systems vendor support personnel did not receive a copy of SPP_URE1's Cyber Security Policy, they 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_URE1's CCAs.	Regarding R1.1, SPP_URE1 revised its Cyber Security Policy to include provisions for emergency situations. Regarding R1.2, SPP_URE1 provided its Cyber Security Policy to its systems vendor. Additionally, SPP_URE1 developed and implemented a new process for making its Cyber Security Policy readily available to its system vendor. The process requires SPP_URE1 to provide its Cyber Security Policy to its vendor on an annual basis, when a change of the policy occurs, or upon request by the vendor. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCRXXXXX	SPP201000329	CIP-004-1	R4.1	During a spot check, SPP RE determined that SPP_URE1 was noncompliant with CIP-004-1 R4.1. Specifically, although SPP_URE1 was reviewing its systems vendor access list annually, it was not reviewing the list quarterly as required by the Standard.	SPP RE has determined that this issue did not pose a serious or substantial risk to the reliability of the Bulk Power System. Although the systems vendor list was not being reviewed quarterly, it was being reviewed annually. Additionally, there is no evidence of any known unauthorized access attempts from any vendor identified on any of SPP_URE1's vendor access lists.	SPP_URE1 updated its process for reviewing its systems vendor access list to include quarterly assessments. As of October 14, 2010, SPP_URE1 reviews all unescorted access rights to Critical Cyber Assets on a quarterly basis. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 1 (SPP_URE1)	NCRXXXXX	SPP201000333	CIP-009-1	R2	During a spot check, SPP RE determined that SPP_URE1 was noncompliant with CIP-009-1 R2. Specifically, SPP_URE1 was required to conduct an exercise of its Critical Cyber Asset Recovery Plan by July 1, 2008, but the exercise was not conducted until April 15, 2009.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Although SPP_URE1 had not exercised its CCA Recovery Plan on the date required, SPP_URE1 did have a recovery plan in place. Further, SPP_URE1's support staff had received comprehensive training on CIP Standards and is very experienced in the support of Critical Cyber Assets and can be reasonably expected to perform the appropriate recovery steps for a wide variety of incidents. Moreover, there have been no events to date requiring activation of the recovery plan.	SPP_URE1's CCA Recovery Plan requires an annual exercise of the plan, which was conducted on April 15, 2009 and prior to the Spot Check. SPP_URE1 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 2 (SPP_URE2)	NCRXXXXX	SPP201000335	EOP-005-1	R6	SPP_URE2 self-reported an issue with Reliability Standard EOP-005-1 R6. SPP_URE2 discovered that one of seven system operators did not have a record of training to the SPP_URE2 System Restoration plan in 2009. SPP_URE2 requires yearly training and the last recorded training for this individual was April 14, 2008. However, as of July 8, 2010, the system operator had been trained.	SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the Bulk Power System. The system operator that did not have a record of training to the SPP_URE2 System Restoration plan in 2009 was a twelve (12) year veteran dispatcher with SPP_URE2 During the time in which the system operator had not been recorded as having received training, no events upon which the training relied occurred. The oversight was promptly noted and the employee received the training. Additionally, all other system operators did have a record of training during this time. Accordingly, SPP RE concluded that the issue had a minimal impact to the reliability of the Bulk Power System.	SPP_URE2 trained the operator in the SPP_URE2 System Restoration plan. Additionally, SPP_URE2 now requires that system operators participate in the SPP restoration drills as part of their job function. These duties are reviewed annually. SPP_URE2 certified that mitigation was complete, and SPP RE verified completion

Attachment A-1

October 31, 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 3 (SPP_URE3)	NCRXXXXX	SPP201000392	CIP-003-1	R6	SPP_URE3 reported in its Self Certification that it was not in full compliance with CIP-003-2 R6 because it did not have a formal change control policy for all Critical Cyber Asset (CCA) hardware, software, and security configurations. Specifically, SPP_URE3 had not established and documented a process for change control and configuration management for adding, modifying, replacing, or removing all CCA hardware or software and it had not implemented supporting configuration management activities.	The SPP RE has determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System. Although SPP_URE3 had not established or documented a process for change control and configuration management for adding, modifying, replacing, or removing all CCA hardware or software, SPP_URE3 did have a Change Control program that it used for changes to its systems hardware and application/database components that were controlled by its vendor. Any changes, additions or upgrades to SPP_URE3 equipment were provided by the vendor to SPP_URE3 and included detailed procedures and configuration changes that explained the effects the new equipment would have on the SPP_URE3's system. Also, SPP_URE3 had been using a spreadsheet to document changes that occurred to its system software, but the procedure of how and when to document changes was not included in SPP_URE3's policy. While the change control program SPP_URE3 used on its SCADA system was not a formal process, it, nonetheless, did document changes in software and hardware that affected an important component in SPP_URE3's system.	To mitigate this issue, SPP_URE3 documented a process and supporting policy for a new change control methodology. This new process and supporting policy considered different types of infrastructure and types of changes (i.e. emergency, low risk, levels of approvals, patches, etc) for CCAs. SPP_URE3 developed applicable templates, forms and change systems to be utilized to support the change control process. Lastly, SPP_URE3 trained all affected SPP_URE3 employees on the new supporting process and policy to ensure that CCA information is identified, protected and classified. SPP_URE3 certified that mitigation was complete, and SPP RE verified completion.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP_URE4) Red Hills Wind Project (Red Hills)	NCRXXXXX	SPP201100460	CIP-001-1	R1	In a Self-Certification, SPP_URE4 indicated that it did not have procedures for the recognition of and for making their operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE4 did not have a physical document addressing sabotage reporting, it stated that it had relied on a third party process for sabotage reporting, and that it used this process for sabotage reporting, along with CIP-001-1, to draft a sabotage document that would comply with CIP-001-1 R1. Because there was a reporting procedure in place, just no documentation of it, the risk to the BPS is minimal.	SPP_URE4 developed an official memo to clarity how to recognize and make its operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the interconnection. SPP_URE4 developed an official procedure to document previously identified SPP_URE4 processes for sabotage reporting, and provided training to its personnel on the procedure. SPP_URE4 certified that mitigation was complete, and SPP RE verified mitigation as complete.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP_URE4) Red Hills Wind Project (Red Hills)	NCRXXXXX	SPP201100461	CIP-001-1	R2	In a Self-Certification, SPP_URE4 indicated that it did not have procedures for communication of information concerning sabotage events to parties in the interconnection.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE4 did not have a physical document addressing sabotage reporting, it stated that it had relied on a third party process for sabotage reporting, and that it used this process for sabotage reporting, along with CIP-001-1, to draft a sabotage document that would comply with CIP-001-1 R2. Because there was a reporting procedure in place, just no documentation of it, the risk to the BPS is minimal.	SPP_URE4 developed an official procedure to document previously identified SPP_URE4' processes for sabotage reporting and provided training to its personnel on the procedure. SPP_URE4 certified that mitigation was complete, and SPP RE verified mitigation as complete.
Southwest Power Pool Regional Entity (SPP RE)	Unidentified Registered Entity 4 (SPP_URE4) Red Hills Wind Project (Red Hills)	NCRXXXXX	SPP201100462	CIP-001-1	R3	In a Self-Certification, SPP_URE4 indicated that it did not provide its operating personnel with sabotage response guidelines for reporting disturbances due to sabotage events.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE4 did not have a physical document addressing sabotage reporting, it stated that it had relied on a third party process for sabotage reporting, and that it used this process for sabotage reporting, along with CIP-001-1, to draft a sabotage document that would comply with CIP-001-1 R3. Because there was a reporting procedure in place, just no documentation of it, the risk to the BPS is minimal.	SPP_URE4 developed an official procedure to document previously identified SPP_URE4' processes for sabotage reporting and provided training to its personnel on the procedure. SPP_URE4 certified that mitigation was complete, and SPP RE verified mitigation as complete.

Attachment A-1

October 31, 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 4 (SPP_URE4) Red Hills Wind Project (Red Hills)	NCRXXXXX	SPP201100463	CIP-001-1	R4	In a Self-Certification, SPP_URE4 indicated that it did not have an official Sabotage Reporting procedure related to establishing communication contacts with the local Federal Bureau of Investigation.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the Bulk Power System (BPS). Although SPP_URE4 did not have a physical document addressing sabotage reporting, it stated that it had relied on a third party process for sabotage reporting, and that it used this process for sabotage reporting, along with CIP-001-1, to draft a sabotage document that would comply with CIP-001-1 R4. Because there was a reporting procedure in place, just no documentation of it, the risk to the BPS is minimal.	SPP_URE4 developed an official procedure to document previously identified SPP_URE4' processes for sabotage reporting and provided training to its personnel on the procedure. SPP_URE4 certified that mitigation was complete, and SPP RE verified mitigation as complete.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1) Rio Grande Electric Co-Op (Rio Grande)	NCRXXXXX	TRE201000159	CIP-001-1	R2	TRE_URE1 did not have a method to disseminate information regarding sabotage to the appropriate parties in the Interconnection. This issue was discovered through a Self-Report.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE1's system owns and operates a small distribution system fed from only two radial lines, thus reducing the risk to the BPS. Also, during the time period of the possible violation no event occurred related to the CIP-001-1.	TRE_URE1 sent new procedures to Texas RE that included a procedure to disseminate information regarding sabotage events, and thus addressing the requirements of CIP-001-1 R2. All mitigation activity has been completed and verified by Texas RE.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (TRE_URE1) Rio Grande Electric Co-Op (Rio Grande)	NCRXXXXX	TRE201000161	CIP-001-1	R4	TRE_URE1 did not have a documented method to contact FBI in regards to recognition of sabotage. This issue was discovered through a Self-Report.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE1's system owns and operates a small distribution system fed from only two radial lines, thus reducing the risk to the BPS. Also, during the time period of the possible violation no event occurred related to the CIP-001-1.	TRE_URE1 sent new procedures to Texas RE dated that included a FBI contact and procedures for contacting the FBI, covering CIP-001-1 R4. All mitigation has been completed and verified by Texas RE.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201100150	CIP-006-1	R1	TRE_URE2 should have timely filed TFEs for some card reader controllers because it did not use anti-virus software and other malicious software prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. Although, some card reader controllers did not use anti-virus software and other malicious software prevention tools, the devices were behind multiple physical security protection boundaries that include at a minimum an outer layer of physical security, at least one CIP compliant card reader system and at least one set of keyed locks.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201100151	CIP-006-1	R1	TRE_URE2 should have timely filed TFEs for some card reader controllers because it did not use anti-virus software and other malicious software prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. Although, some card reader controllers did not use anti-virus software and other malicious software prevention tools, the devices were behind multiple physical security protection boundaries that include at a minimum an outer layer of physical security, at least one CIP compliant card reader system and at least one set of keyed locks.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201000318	CIP-007-1	R4	TRE_URE2 should have timely filed TFEs for some card reader controllers because it did not use anti-virus software and other malicious software prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. The Cyber Assets which do not have an anti-virus and other malicious software prevention tools also do not have operating systems installed on the devices. The lack of an operating system not only prevents anti-virus software from being loaded onto the devices, this also prevents any virus and/or malware from infecting the devices. Without the ability to become infected by a virus or malware, there is no actual risk to the bulk power system.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.

Attachment A-1

October 31, 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
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201000319	CIP-007-1	R5	TRE_URE2 should have timely filed TFEs on card reader controllers because the devices do not have the ability to enforce the password length; alpha, numeric and special characters; and the annual password change. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. The Cyber Assets which do not enforce passwords length, complexity or require annual change also do not have the ability to allow users to log into the devices. The CIP standard's requirement to use passwords is intended to prevent unauthorized system access. Therefore there is no risk to bulk power system from an unauthorized system access, due to the systems inability to grant system access.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201000357	CIP-007-1	R4	TRE_URE2 should have timely filed TFEs on card reader controllers because it did not use anti-virus software and other malicious software prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeters. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. The Cyber Assets which do not have an anti-virus and other malicious software prevention tools also do not have operating systems installed on the devices. The lack of an operating system not only prevents anti-virus software from being loaded onto the devices, this also prevents any virus and/or malware from infecting the devices. Without the ability to become infected by a virus or malware, there is no actual risk to the bulk power system.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 2 (TRE_URE2)	NCRXXXXX	TRE201000358	CIP-007-1	R5	TRE_URE2 should have timely filed TFEs on card reader controllers because the devices do not have the ability to enforce the password length; alpha, numeric and special characters; and the annual password change. TRE_URE2 failed to file TFEs until May 17, 2010. This issue was discovered through a Self-Report.	This violation does not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system. The Cyber Assets which do not enforce passwords length, complexity or require annual change also do not have the ability to allow users to log into the devices. The CIP standard's requirement to use passwords is intended to prevent unauthorized system access. Therefore there is no risk to bulk power system from an unauthorized system access, due to the systems inability to grant system access.	Mitigation plan was completed and verified. Filing of TFEs on May 17, 2010 addressed the issue.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 3 (TRE_URE3)	NCRXXXXX	TRE201000287	IRO-004-1	R4	TRE_URE3 failed to submit a day-ahead resource plan for its share of a facility by 16:00 (day-ahead) for the next operating day. Regional rules require that this information be submitted by 16:00 for the day-ahead. This issue was discovered through a Self-Report.	Texas RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the bulk power system because this was a single occurrence mitigated in real-time by manual processes. Once the error was discovered, TRE_URE3's resource plan was immediately submitted. Furthermore, despite the failure to submit the resource plan, ERCOT ISO was able to manually enter TRE_URE3's day-ahead information to timely perform stability limit calculations.	TRE_URE3 has since updated its procedures to include additional checks and verifications that a resource plan has been submitted and received.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4) Bandera Electric Co Op (Bandera Electric)	NCRXXXXX	TRE201000306	CIP-001-1	R1	TRE_URE4's sabotage procedures did not address the requirements of CIP-001-1 R1 and were not provided to operating personnel. Adequate procedures were provided after the registration date. This issue was discovered through a Self-Certification.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE4 had sabotage-related procedures in place that addressed reporting of hazardous conditions although the procedures did not fully address the requirements of this Standard. This reduced the risk to the BPS. Also, operating personnel were verbally told to report suspected sabotage to the appropriate authorities.	Mitigation plan was completed and verified. Latest procedures address the requirement of this Standard and were supplied to personnel.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4) Bandera Electric Co Op (Bandera Electric)	NCRXXXXX	TRE201000307	CIP-001-1	R2	TRE_URE4's sabotage procedures did not contain adequate provisions for the communication of information concerning sabotage events to appropriate parties in the Interconnection. Latest procedures were adequate. This issue was discovered through a Self-Certification.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE4 had sabotage-related procedures in place, that addressed reporting hazardous conditions although the procedures did not fully address the requirements of this Standard. This reduced the risk to the BPS. Also, operating personnel were verbally told to report suspected sabotage to the appropriate authorities.	Mitigation plan was completed and verified. TRE_URE4's latest procedures contain provisions for the communication of information concerning sabotage events to appropriate parties in the interconnection.

Attachment A-1

October 31, 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
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4) Bandera Electric Co Op (Bandera Electric)	NCRXXXXX	TRE201000308	CIP-001-1	R3	TRE_URE4's sabotage procedures did not contain adequate response guidelines. The latest procedures were found to be adequate by Texas RE. This issue was discovered through a Self-Certification.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE4 had sabotage-related procedures in place that addressed reporting of hazardous conditions although the procedures did not fully meet the requirements of this Standard. These procedures reduced the risk to the BPS. Also, operating personnel were verbally told to report suspected sabotage to the appropriate authorities.	Mitigation plan was completed and verified. Latest procedures contain adequate response guidelines.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 4 (TRE_URE4) Bandera Electric Co Op (Bandera Electric)	NCRXXXXX	TRE201000165	CIP-001-1	R4	TRE_URE4's sabotage procedures did not adequately address reporting procedures or include a FBI contact. This issue was discovered through a Self Certification.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system (BPS) because TRE_URE4 had sabotage-related procedures in place that addressed reporting of hazardous conditions although the procedures did not fully meet the requirements of this Standard. These procedures reduced the risk to the BPS. Also, operating personnel were verbally told to report suspected sabotage to the appropriate authorities.	Mitigation plan was completed and verified. Latest procedures contain FBI contact information.
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 5 (TRE_URE5) Electric Reliability Council of Texas, Inc. (ERCOT)	NCRXXXXX	TRE201000351	CIP-003-2	R2.3	As a result of an Audit, Texas RE determined that TRE_URE5's delegation of authority for specific actions to a named delegate, specifically approval of exceptions to its security policy did not include the name of the delegate, only the title and date of designation.	This issue did not pose a serious or substantial risk and posed a minimal potential and actual risk to the bulk power system because although the document did not explicitly list the name, the title was listed. During the compliance period, that title/position was held by the same person. Although that person changed official job titles, the entity presented other documents and emails that demonstrated that that person was the person being referred to in the delegation of authority.	TRE_URE5 revised the designation of authority so that it was consolidated into one document and includes delegate's name, title, and date of designation. TRE_URE5 also revised the 'Exceptions' form to include the name of the authorized delegate, as well as their title. This will cause any change of authorized delegate to require a change to the forms as well.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1) Northern California Power Agency (NCPA)	NCRXXXXX	WECC201102908	CIP-002-3	R4	During an annual internal review of the CIP Standards, WECC_URE1 found a discrepancy in its procedures. Specifically, WECC_URE1's senior manager failed to review the Risk Based Assessment Methodology (RBAM) for the 2010 calendar year. WECC_URE1 notes that versions 1 and 2 of the standard required an entity to approve annually the list of Critical Assets and the list of Critical Cyber Assets. However, when Version 3 of the standard became effective, the requirement included an annual review and approval of the RBAM in addition to annually approving the list of Critical Assets and the list of Critical Cyber Assets.	Although WECC_URE1 did not have a signed and dated record of the senior manager or delegate(s)'s annual approval of its 2010 Risk Based Assessment Methodology (RBAM), WECC_URE1's CIP Senior Manager had approved the Critical Asset and Critical Cyber Asset lists for calendar year 2010. While WECC_URE1 failed to review the RBAM in the calendar year 2010, WECC_URE1 created its RBAM in 2009, and annually approved the RBAM in 2009 and again in 2011. Additionally, WECC_URE1's list of Critical Assets and Critical Cyber Assets is null, which had not changed from years prior. Therefore, WECC_URE1's failure to update its procedure to include the annual approval of the RBAM did not negatively impact the BPS because the lists of Critical Assets and Critical Cyber Assets for WECC_URE1 were and remained null for the year. For these reasons, WECC determined this issue posed a minimal risk to the reliability of the BPS.	WECC_URE1 updated the annual approval procedure to include an annual review and approval of its RBAM by the CIP Senior Manager. Additionally, WECC_URE1 has hired a third-party consultant to validate the RBAM.

Document Content(s)