Federal Energy Regulatory Commission
Washington, D.C. 20426

June 30, 2021

Release Letter
FOIA No. FY19-30

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 letters dated June 24, 2021, the submitter and certain concerned Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notices of Penalty associated with Docket Nos. RC12-11; NP11-266; and NP11-270, along with the names of certain relevant UREs and associated dockets 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 documents are enclosed.

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

[1] 5 U.S.C. § 552 (2018).

[2] These dockets involved multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to those UREs for whom FERC determined that disclosure of their identities was appropriate.

to discuss any aspect of your request, you may contact Assistant United States Attorney April D. Seabrook by email at april.seabrook@usdoj.gov, by phone at (202) 252-2525, or by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

Sarah Venuto

Digitally signed by Sarah Venuto
Date: 2021.06.30 14:12:36 -04'00'

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

NP11-270

September 30, 2011

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

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP11-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Spreadsheet Notice of Penalty[1] (Spreadsheet NOP) in Attachment A regarding 21 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]

The Spreadsheet NOP resolves 75 violations[5] of 19 Reliability Standards. In order to be a candidate for inclusion in the Spreadsheet NOP, the violations are those that had a minimal or moderate impact on the reliability of the bulk power system (BPS). In all cases, the NOP sets forth whether the violations have been mitigated, certified by the respective Registered Entities as mitigated, and verified by the Regional Entity as having been mitigated.

---

[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 violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

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

The violations at issue in the Spreadsheet NOP are being filed with the Commission because the Regional Entities have respectively entered into settlement agreements with, or have issued Notices of Confirmed Violations (NOCVs) to, the Registered Entities identified in Attachment A and have resolved all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and findings of the enforceable violation of the Reliability Standards identified in Attachment A. As designated in the attached spreadsheet, some of the Registered Entities have admitted to the violations, while the others have indicated that they neither admit nor deny the violations and have agreed to the proposed penalty as stated in Attachment A or did not dispute the violations and proposed penalty amount stated in Attachment A, in addition to other remedies and mitigation actions to mitigate the instant violations and ensure future compliance with the Reliability Standards. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

As discussed below, this Spreadsheet NOP resolves 75 violations. NERC respectfully requests that the Commission accept this Spreadsheet NOP.

Statement of Findings Underlying the Alleged Violations

The descriptions of the violations 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 and penalties 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 Notice of Penalty is set forth in Attachment A.

Text of the Reliability Standards at issue in the Spreadsheet NOP may be found on NERC's web site at http://www.nerc.com/page.php?cid=2|20. For each respective violation, the Reliability Standard Requirement at issue and the applicable Violation Risk Factor are set forth in Attachment A.

In approving the Spreadsheet NOP, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue. In each of the violations included in Attachment A, unless otherwise detailed within the Spreadsheet NOP, the Registered Entities were cooperative throughout the compliance enforcement process; there was no evidence of any attempt to conceal a violation or evidence of intent to do so. In accordance with the Guidance Order issued by FERC concerning treatment of repeat violations and violations of corporate affiliates, the violation history for the Registered Entities and

affiliated entities who share a common corporate compliance program is detailed in Attachment A when that history includes violations of the same or similar Standard. Additional mitigating, aggravating, or extenuating circumstances beyond those listed above are detailed in Attachment A.

Status of Mitigation[6]

The mitigation activities are described in Attachment A for each respective violation. Information also is provided regarding the dates of Registered Entity certification and the Regional Entity verification of such completion where applicable.

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the violations in the Spreadsheet NOP on August 2, 2011 and September 19, 2011. The NERC BOTCC approved the violations in the Spreadsheet NOP, including the Regional Entities' imposition of financial penalties as reflected in Attachment A, 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 violations at issue.

Pursuant to Order No. 693, the penalties will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review any specific penalty, upon final determination by FERC.

[6] *See* 18 C.F.R § 39.7(d)(7).
[7] *See* 18 C.F.R § 39.7(d)(4).
[8] *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).

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 violations and confidential information regarding critical energy infrastructure.

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

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

Attachments to be included as Part of this Spreadsheet Notice of Penalty

The attachments to be included as part of this Spreadsheet Notice of Penalty are the following documents and material:

a) Spreadsheet Notice of Penalty, included as Attachment A;

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

c) Violation Risk Factor Revision History Applicable to the Spreadsheet Notice of Penalty, included as Attachment C.

A Form of Notice Suitable for Publication[9]

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

[9] *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 Spreadsheet NOP:

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.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Spreadsheet Notice of Penalty as compliant with its rules, regulations and orders.

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

Spreadsheet Notice of Penalty
(Included in a Separate Document)

NERC

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR SEPTEMBER 2011 SPREADSHEET NOP INFORMATIONAL FILING

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 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 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

Violation Risk Factor Revision History Applicable to the Spreadsheet Notice of Penalty

ATTACHMENT C

Violation Risk Factor Revision History Applicable to the Spreadsheet Notice of Penalty

Some of the Violation Risk Factors in the Notice of Penalty spreadsheet can be attributed to the violation being assessed at a main requirement or sub-requirement level. Also, some of the Violation Risk Factors were assigned at the time of discovery. Over time, NERC has filed new Violation Risk Factors, which have been approved by FERC.

- When NERC filed Violation Risk Factors (VRF) it originally assigned CIP-002-1 R1 and R1.2 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on January 27, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-002-1 R1 and R1.2 were in effect from June 18, 2007 until January 27, 2009 when the Medium VRFs became effective. CIP-002-1 R1 and R1.2 are each assigned a Medium VRF and CIP-002-1 R1.1, R1.2.1, R1.2.2, R1.2.3, R1.2.4, R1.2.5, R1.2.6 and R1.2.7 are each assigned a Lower VRF.

- When NERC filed VRFs it originally assigned CIP-002-1 R2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Lower VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective.

- When NERC filed VRFs it originally assigned CIP-002-1 R3 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on January 27, 2009, the Commission approved the modified High VRF. Therefore, the Medium VRF for CIP-002-1 R3 was in effect from June 18, 2007 until January 27, 2009 when the High VRF became effective. CIP-002-1 R3 is assigned a High VRF and CIP-002-1 R3.1, R3.2 and R3.3 are each assigned a Lower VRF.

- CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a Lower VRF; R2.1, R2.2 and R2.2.4 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

- CIP-004-1 R3 has a Medium VRF; R3.1, R3.2 and R3.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-004-1 R3 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R3 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

- CIP-004-1 R4 and R4.1 each have a Lower VRF; R4.2 has a Medium VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective. The VRFs for CIP-004-3 R4 were not changed when CIP-004-3 went into effect on October 1, 2010.

- CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a Medium VRF; R1.6 has a Lower VRF. CIP-005-1 R1.1, R1.2, R1.3, R1.4 and R1.5 When NERC filed VRFs it originally assigned CIP-005-1 R1.1, R1.2, R1.3, R1.4 and R1.5 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009 the Commission approved the modified Medium VRFs for CIP-005-1 R1.1, R1.2, R1.3, and R1.4 and on August 20, 2009, the Commission approved the modified Medium VRF for CIP-005-1 R1.5. Therefore, the Lower VRFs for CIP-005-1 R1.1, R1.2, R1.3, and R1.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective and the Lower VRF for CIP-005-1 R1.5 was in effect from June 18, 2007 until August 20, 2009 when the Medium VRF became effective.

- CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a Medium VRF; R2.5 and its sub-requirements and R2.6 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-005-1 R2 and R2.4 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRFs for CIP-005-1 R2 and R2.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

- CIP-005-1 R3, R3.1 and R3.2 each have a Medium VRFs. When NERC filed VRFs it originally assigned CIP-005-1 R3, R3.1 and R3.2 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the

Lower VRFs for CIP-005-1 R3, R3.1 and R3.2 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

- CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a Medium VRF; R1.7, R1.8 and R1.9 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective.

- CIP-006-1 R6 and R6.1 each have a Medium VRF and CIP-006-1 R6.2 and R6.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-006-1 R6.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R6.1 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective.

- When NERC filed VRFs it originally assigned CIP-007-1 R2 and R2.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R2 and R2.3 were in effect from June 18, 2007 until February 2, 2009, when the Medium VRFs became effective.

- CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF. When NERC originally filed VRFs it originally assigned CIP-005-1 R5.1 and R5.3.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on August 20, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-005-1 R5.1 and R5.3.3 were in effect from June 18, 2007 until August 20, 2009, when the Medium VRFs became effective. When NERC originally filed VRFs it originally assigned CIP-005-1 R5.1.3, R5.2.1 and R5.2.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-005-1 R5.1.3, R5.2.1 and R5.2.3 were in effect from June 18, 2007 until February 2, 2009, when the Medium VRFs became effective. The VRFs for CIP-007-2 R5 were not changed when CIP-007-2 went into effect on April 1, 2010.

- CIP-007-1 R1 has a Medium VRF and CIP-007-1 R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-007-1 R1.1 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-007-1 R1.1 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

- CIP-007-1 R6, R6.4 and R6.5 each have a Lower VRF and R6.1, R6.2 and R6.3 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-007-1 R6.1, R6.2 and R6.3 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-007-1 R6.1, R6.2 and R6.3 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

- When NERC filed VRFs it originally assigned EOP-008-0 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on February 6, 2008, the Commission approved the modified High VRF. Therefore, the Medium VRF for EOP-008-0 R1 was in effect from June 18, 2007 until February 6, 2008 when the High VRF became effective.

- FAC-008-1 R1, R1.3 and R1.3.5 each have a Lower VRF; R1.1, R1.2, R1.2.1, R1.2.2, R1.3.1-4 each have a Medium VRF. When NERC filed VRFs it originally assigned FAC-008-1 R1.1, R1.2, R1.2.1 and R1.2.2 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on February 6, 2008, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for FAC-008-1 R1.1, R1.2, R1.2.1 and R1.2.2 were in effect from June 18, 2007 until February 6, 2008 when the Medium VRFs became effective.

- When NERC filed VRFs for PRC-001-1, NERC originally assigned a Medium VRF to PRC-001-1 R1. In the Commission's May 18, 2007 Order on Violation Risk Factors, the Commission approved the VRF as filed but directed modifications. On June 1, 2007, NERC filed a modified High VRF for PRC-001-1 R1 for approval. On August 9, 2007, the Commission issued an Order approving the modified VRF. Therefore, the Medium VRF was in effect from June 18, 2007 until August 9, 2007 and the High VRF has been in effect since August 9, 2007.

- When NERC filed VRFs it originally assigned PRC-001-1 R3 a High VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified <blank> VRF and on August 9, 2007, the Commission approved the modified <blank> VRF. Therefore, the High

VRF for PRC-001-1 R3 was in effect from June 18, 2007 until August 9, 2007 when the <blank> VRF became effective.

- When NERC filed VRF it originally assigned PRC-005-1 R1 a Medium VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified High VRF and on August 9, 2007, the Commission approved the modified High VRF. Therefore, the Medium VRF for PRC-005-1 R1 was in effect from June 18, 2007 until August 9, 2007 when the High VRF became effective.

- PRC-005-1 R2 has a Lower VRF; R2.1 and R2.2 each have a High VRF. During a final review of the standards subsequent to the March 23, 2007 filing of the Version 1 VRFs, NERC identified that some standards requirements were missing VRFs; one of these include PRC-005-1 R2.1. On May 4, 2007, NERC assigned PRC-005 R2.1 a High VRF. In the Commission's June 26, 2007 Order on Violation Risk Factors, the Commission approved the PRC-005-1 R2.1 High VRF as filed. Therefore, the High VRF was in effect from June 26, 2007.

NERC

Attachment d

Notice of Filing

ATTACHMENT D

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. NP11-___-000

NOTICE OF FILING
September 30, 2011

Take notice that on September 30, 2011, the North American Electric Reliability Corporation (NERC) filed a Spreadsheet Notice of Penalty regarding twenty-one (21) Registered Entities in three (3) 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
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* Corporation (RFC)	Armstrong Energy Limited Partnership, LLLP (Armstrong Energy)	NCR00211	RFC201000408	Settlement Agreement	During a compliance audit from June 14, 2010 through June 25, 2010 (Audit), Reliability*First* , determined that Armstrong Energy, as a Generator Owner, failed to include a basis for any of its maintenance and testing intervals in its Protection System maintenance and testing program in effect from August 5, 2008 to August 28, 2008 (Program). In addition, the Program did not include maintenance and testing intervals or a summary of maintenance and testing procedures for communications systems. On August 28, 2008, Armstrong Energy issued a new Protection System maintenance and testing program to replace the August 5, 2008 Program.	PRC-005-1	R1	High	Severe	Reliability*First* determined that this violation posed a moderate but did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Program was in place for less than one battery testing cycle and the duration of the violation was for less than one month. Armstrong Energy missed no maintenance and testing intervals as a result of the violation. In addition, Armstrong Energy has alarms in place to detect abnormal conditions for its voltage sensing devices, relays and station batteries and these alarms did not sound during the period of the violation. Furthermore, Armstrong Energy conducts daily walk down inspections of its plant, including all relay and battery rooms, to check for faults and Armstrong Energy detected no faults during the time period of the violation.	8/5/2008	8/28/2008	$10,000 (for RFC201000408 and RFC201000409)	Compliance Audit	On August 17, 2011, Armstrong Energy submitted a mitigation plan to address the violation of PRC-005-1 R1. Armstrong Energy took the following action to mitigate the violation. Armstrong Energy issued a new Protection System maintenance and testing program on August 28, 2008, which included communication systems and the basis for all maintenance and testing intervals.	8/28/2008	8/8/2011	Admits	Although Reliability*First* reviewed a previous violation of PRC-005-1 R2 by Armstrong Energy's affiliate, Troy Energy LLC, Reliability*First* determined that this prior violation should not serve as a basis for aggravating the penalty since Armstrong Energy's violation of PRC-005-1 R1 preceded Troy's violation. Moreover, there was nothing in the record to suggest that broader corporate issues were implicated. Reliability*First* considered Armstrong Energy's internal compliance program (ICP) as a mitigating factor in assessing the penalty.
Reliability*First* Corporation (RFC)	Armstrong Energy Limited Partnership, LLLP (Armstrong Energy)	NCR00211	RFC201000409	Settlement Agreement	During a compliance audit from June 14, 2010 through June 25, 2010 (Audit), Reliability*First* determined that while Armstrong Energy, as a Generator Owner, provided a Facility Ratings Methodology (Methodology), the Methodology did not include transmission conductors in its scope, as required by the Standard. In addition, the Methodology did not include Normal and Emergency Ratings for transmission conductors in its scope.	FAC-008-1	R1	Medium	Severe	Reliability*First* determined that this violation posed a moderate but did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Armstrong Energy provided the manufacturer's ratings for the transmission conductors at the Audit, and did not deviate from the manufacturer's ratings when it amended its Methodology to include transmission conductors and their Normal and Emergency Ratings.	8/5/2008	7/12/2010	$10,000 (for RFC201000408 and RFC201000409)	Compliance Audit	On March 17, 2011, Armstrong Energy submitted a mitigation plan to address the violation of FAC-008-1 R1.2. Armstrong Energy took the following action to mitigate the violation. Armstrong Energy amended its Methodology to include transmission conductors, including their Normal and Emergency Ratings.	7/12/2010	8/5/2011	Admits	Although Reliability*First* reviewed a previous violation of PRC-005-1 R2 by Armstrong Energy's affiliate, Troy Energy LLC, Reliability*First* determined that this prior violation should not serve as a basis for aggravating the penalty since Armstrong Energy's violation is not the same or similar to the standard. Moreover, there was nothing in the record to suggest that broader corporate issues were implicated. Reliability*First* considered Armstrong Energy's internal compliance program (ICP) as a mitigating factor in assessing the penalty.
Reliability*First* Corporation (RFC)	Buckeye Power, Inc. (Buckeye Power)	NCR00700	RFC201000654	Settlement Agreement	From September 13, 2010 to September 28, 2010, Reliability*First* conducted a compliance audit of Buckeye Power, during which Reliability*First* discovered a violation of PRC-005-1 R1. Reliability*First* determined that Buckeye Power, as a Generator Owner that owns a generation Protection System, did not include maintenance and testing intervals for current and voltage sensing devices in its Protection System maintenance and testing program, violating PRC-005-1 R1.1. Additionally, Reliability*First* determined that Buckeye Power's Protection System maintenance and testing program did not have a summary of maintenance and testing procedures for current and voltage sensing devices, violating PRC-005-1 R1.2. This violation pertained to all of Buckeye Power's 327 voltage and current sensing devices constituting 27.6% of Buckeye Power's 1,186 total Protection System devices.	PRC-005-1	R1	High	Moderate	In considering the risk to the reliability of the bulk power system (BPS), Reliability*First* considered the fact that Buckeye Power did not have any redundant or back up protections in place for the current and voltage sensing devices. Buckeye Power was also unable to provide evidence of prior testing to demonstrate that the current and voltage sensing devices were fully functional and within specifications prior to the missed intervals. Reliability*First* considered this in light of the important function fulfilled by current and voltage sensing devices. Current and voltage sensing devices, specifically the current transformers and voltage transformers, provide electrical information directly to the relays regarding events and operations on the system. In order to detect a fault, the relays require accurate information from the current and voltage transformers as input. Without input from these devices, the relays would not have information necessary to react correctly (e.g., resulting in a failure to trip or a false trip by the relay). Reliability*First* considered this important function of current and voltage sensing devices in determining the risk to the reliability of the BPS resulting from Buckeye Power's failure to test these devices. Buckeye Power continues to test these devices to confirm that all devices are currently fully functional and within specifications and will complete this testing on December 31, 2011. Buckeye Power has tested 61 of the 327 current and voltage sensing devices and has confirmed that those devices were fully functional and within specifications. Reliability*First* considered these limited results as mitigating the risk. Reliability*First* also considered that the risk was mitigated by the fact that Buckeye Power monitored its system throughout the duration of the violation and represents that no generating unit outage, equipment failure, or confirmation of any current and voltage sensing misoperation occurred. In light of the nature of the violation, offset by the aforementioned mitigating factors, Reliability*First* determined that this violation posed a moderate risk to the reliability of the BPS.	June 18, 2007, the date of mandatory compliance.	December 31, 2011, the date on which Buckeye Power will complete its maintenance and testing of current and voltage sensing devices.	$25,000 (for RFC201000654)	Compliance Audit	Buckeye Power added intervals and their basis with a summary of the requisite maintenance and testing procedures for its current and voltage sensing devices to its maintenance and testing program. Buckeye Power has agreed to complete the maintenance and testing of these devices by December 31, 2011.	12/31/2011 (approved date)	TBD	Agrees and Stipulates to the Facts	Reliability*First* considered Buckeye Power's established, formal program for internal compliance as a mitigating factor. The internal compliance program resides within Buckeye Power's Power Supply division and was widely disseminated to all individuals within this division through small workshops, training by consultants, e-mails, meetings and in person. The program was supervised by three senior staff members who report to the Chief Operating Officer, who reports to the Chief Executive Officer and President. Buckeye Power's self-assessment of its internal compliance program resulted in expanding the scope of compliance activities to include more staff, including an additional consultant.
Reliability*First* Corporation (RFC)	City of Dover, Ohio (Dover)	NCR08007	RFC201000461	Settlement Agreement	During a Compliance Audit conducted from June 14, 2010 to June 25, 2010, Reliability*First* found that Dover, as a DP, failed to have: (a) a maintenance and testing program ("Program") that included maintenance and testing intervals and the basis for those intervals for 100% of its 48 voltage and current sensing devices; and (b) a summary of maintenance and testing procedures for 100% of its 48 voltage and current sensing devices and 100% of its battery system, which consists of 60 individual cells.	PRC-005-1	R1	High	Severe	In light of the nature of the violation, offset by the mitigating factors, Reliability*First* determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS). The risk was mitigated due to these factors: (a) Dover's Protection System relays, battery systems, and voltage and current sensing devices were inspected monthly; (b) Dover's substation and 30 of Dover's voltage and current sensing devices are monitored by the SCADA system and state estimator, neither of which has shown abnormal conditions with Dover's voltage and current sensing devices; (c) the substation is inspected at least monthly by Dover personnel; and (d) personnel from the entity with which Dover contracts performed visual inspections of all meters, potential indicating lights, and any alarm functions during the time period of the violation, and this personnel has not reported any problems.	June 27, 2007, date Dover registered with NERC Compliance Registry.	June 7, 2011, the date Dover revised its Program to include maintenance and testing intervals for its voltage and current sensing devices.	$10,000 (Settlement for RFC201000461)	Compliance Audit	Dover included, in its Program, a six year interval, and its basis, for its voltage and current sensing devices. Additionally, Dover acquired a summary of maintenance and testing procedures for its voltage and current sensing devices and batteries from the entity with which Dover contracts to perform maintenance and testing on its Protection System devices.	7/12/2011	8/3/2011	Agrees and Stipulates to the Facts	Reliability*First* considered certain aspects of Dover's internal compliance program as mitigating factors. For instance, Dover has an internal compliance program to develop and update policies and procedures in order to comply with Reliability Standards. Dover will modify the internal compliance program on an annual basis or more frequently if necessary. Dover distributes its internal compliance policies and procedures to its personnel. Dover also designated its Electric Generation Superintendent as its reliability officer.
Reliability*First* Corporation (RFC)	Michigan Public Power Agency (MPPA)	NCR00822	RFC200900219	Settlement Agreement	During a Compliance Audit conducted from June 14, 2010 through June 25, 2010, MPPA did not submit documentation of a protection system maintenance and testing program for its member city, City of Holland Board of Public Works (Holland)'s 48th Street Peaking Station (48th Street Peaking Station). MPPA incorrectly believed, since its registration, that PRC-005-1 R1 was not applicable because MPPA incorrectly believed that 48th Street Peaking Station was not part of the bulk power system. As a result, MPPA did not assemble documentation of its protection system maintenance and testing program prior to the Compliance Audit. Specifically, MPPA did not produce a comprehensive document that included maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for protection system devices. MPPA, as a GO, violated PRC-005-1 R1 by failing to produce sufficient documentation of a protection system maintenance and testing program for the 48th Street Peaking Station.	PRC-005-1	R1	High	High	Reliability*First* found that this violation posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS) because there are multiple protective relays and breakers between the 48th Street Peaking Station and Holland's interconnection at the Black River switching station, which is configured to minimize the risk to the BPS in the event of a possible failure at the 48th Street Peaking Station. In addition, MPPA represents that no relay malfunctions occurred at the 48th Street Peaking Station since the relays' installation, and all relays were found to be in good condition upon testing in 2008.	June 18, 2007, the date MPPA registered with NERC Compliance Registry.	May 26, 2010, the date MPPA adopted a documented protection system maintenance and testing program for the 48th Street Peaking Station.	$12,000 (for RFC200900219; RFC200900220; RFC200900221; and RFC200900222)	Compliance Audit	MPPA documented and adopted a protection system maintenance and testing program that included maintenance and testing intervals and their basis, and a summary of maintenance and testing procedures.	5/26/2010	9/13/2011	Neither Admits nor Denies	Reliability*First* considered certain aspects of MPPA's compliance program as mitigating factors in the penalty determination. For example, MPPA's Compliance Manager and Senior Engineer meet with key member personnel on an annual basis. Additionally, MPPA holds workshops to advise both member and non-member cities on compliance issues. MPPA's compliance program has the support and involvement of senior management, including MPPA's General Manager. The Compliance Manager reports directly to the General Manager and the two are in regular and frequent contact. In addition, the Compliance Manager regularly attends meetings of the Board of Commissioners (MPPA's governing body) and reports on the compliance program as part of the regular agenda. MPPA's Compliance Policy requires ongoing internal auditing and monitoring of the implementation of its compliance program and MPPA has hired consultants to conduct audits. MPPA's General Manager has issued guidelines indicating that lack of compliance with the statutory and regulatory standards will affect employee compensation and opportunities for promotion.
Reliability*First* Corporation (RFC)	Michigan Public Power Agency (MPPA)	NCR00822	RFC200900220	Settlement Agreement	During the Compliance Audit, MPPA submitted maintenance and testing documentation to support the compliance of Holland's Generators 7 and 8 with PRC-005-1, R2, for the test year 2008, but did not submit complete maintenance and testing documentation sufficient to meet Reliability*First*'s satisfaction to support the compliance of Holland's Generators 7 and 8 with PRC-005-1 R2 for the test year 2004. Holland's Generators 7 and 8 are located at the 48th Street Peaking Station. Reliability*First* was unable to verify the timely completion of a four-year maintenance and testing interval for some of the protection system devices at Holland's Generators 7 and 8, due to incomplete maintenance and testing documentation for test year 2004. Specifically, for Generator 7, which contains 20 relays, MPPA produced documentation of 2004 work orders but no documentation that MPPA tested relays in 2004. For Generator 8, which also contains 20 relays, MPPA produced documentation that it tested 15 relays in 2004. MPPA, as a GO, violated PRC-005-1 R2 by failing to provide sufficient evidence that all of the protection system devices at Holland's Generators 7 and 8 were tested within the defined intervals of its protection system maintenance and testing program.	PRC-005-1	R2	High	Severe	Reliability*First* found that this violation posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS) because there are multiple protective relays and breakers between the 48th Street peaking Station and Holland's interconnection at the Black River switching station, which is configured to minimize the risk to the BPS in the event of a possible failure at the 48th Street Peaking Station. In addition, MPPA represents that all relays at the 48th Street Peaking Station functioned and were in good condition upon testing in October 2008. MPPA represents that no relay malfunctions occurred at the 48th Street Peaking Station since the relays' installation.	June 18, 2007, the date MPPA registered with NERC Compliance Registry.	October 22, 2010, date MPPA completed maintenance and testing for the protection system devices at issue.	$12,000 (for RFC200900219; RFC200900220; RFC200900221; and RFC200900222)	Compliance Audit	MPPA maintained and tested the relays at issue in the alleged violation in October 2008. MPPA documented and adopted a protection system maintenance and testing program that included maintenance and testing intervals and their basis, and a summary of maintenance and testing procedures. MPPA confirmed that all maintenance and testing was current and in accordance with its protection system maintenance and testing program.	5/26/2010	9/13/2011	Neither Admits nor Denies	Reliability*First* considered certain aspects of MPPA's compliance program as mitigating factors in the penalty determination. For example, MPPA's Compliance Manager and Senior Engineer meet with key member personnel on an annual basis. Additionally, MPPA holds workshops to advise both member and non-member cities on compliance issues. MPPA's compliance program has the support and involvement of senior management, including MPPA's General Manager. The Compliance Manager reports directly to the General Manager and the two are in regular and frequent contact. In addition, the Compliance Manager regularly attends meetings of the Board of Commissioners (MPPA's governing body) and reports on the compliance program as part of the regular agenda. MPPA's Compliance Policy requires ongoing internal auditing and monitoring of the implementation of its compliance program and MPPA has hired consultants to conduct audits. MPPA's General Manager has issued guidelines indicating that lack of compliance with the statutory and regulatory standards will affect employee compensation and opportunities for promotion.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* Corporation (RFC)	Michigan Public Power Agency (MPPA)	NCR00822	RFC200900221	Settlement Agreement	MPPA did not have a documented facility ratings methodology for the 48th Street Peaking Station as it incorrectly believed that the 48th Street Peaking Station, part of Holland's generation system, was not part of the bulk power system. On May 1, 2009, MPPA submitted a documented Facilities Ratings Methodology to Reliability*First* , which was adopted on April 20, 2009. MPPA, as a GO, violated FAC-008-1 R1 by failing to have a documented Facility Ratings Methodology for the 48th Street Peaking Station.	FAC-008-1	R1	Medium	Severe	Reliability*First* found that this violation posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS) because MPPA represents that it did have facility ratings for the 48th Street Peaking Station, and upon development and application of the facility ratings methodology, MPPA confirmed that it had correctly identified the most limiting element in the facility ratings in place during the time period of the alleged violation. In addition, there are no instances since the installation of the 48th Street Peaking Station of thermal overloads or exceeding of established facility ratings.	June 18, 2007, the date MPPA registered with NERC Compliance Registry.	April 20, 2009, the date MPPA adopted a documented facility ratings methodology.	$12,000 (for RFC200900219; RFC200900220; RFC200900221; and RFC200900222)	Compliance Audit	MPPA adopted a facility ratings methodology and provided it to Reliability*First* . MPPA then retained a technical consultant to further enhance its facility ratings methodology to include more background information and descriptions and adopted the enhanced facility ratings methodology.	5/28/2010	9/13/2011	Neither Admits nor Denies	Reliability*First* considered certain aspects of MPPA's compliance program as mitigating factors in the penalty determination. For example, MPPA's Compliance Manager and Senior Engineer meet with key member personnel on an annual basis. Additionally, MPPA holds workshops to advise both member and non-member cities on compliance issues. MPPA's compliance program has the support and involvement of senior management, including MPPA's General Manager. The Compliance Manager reports directly to the General Manager and the two are in regular and frequent contact. In addition, the Compliance Manager regularly attends meetings of the Board of Commissioners (MPPA's governing body) and reports on the compliance program as part of the regular agenda. MPPA's Compliance Policy requires ongoing internal auditing and monitoring of the implementation of its compliance program and MPPA has hired consultants to conduct audits. MPPA's General Manager has issued guidelines indicating that lack of compliance with the statutory and regulatory standards will affect employee compensation and opportunities for promotion.
Reliability*First* Corporation (RFC)	Michigan Public Power Agency (MPPA)	NCR00822	RFC200900222	Settlement Agreement	During the Compliance Audit, Reliability*First* determined that the facility ratings for the 48th Street Peaking Station were not consistent with an associated facility ratings methodology because there was no facility ratings methodology. MPPA's compliance procedure mistakenly concluded that FAC-009-1 R1 was not applicable to Holland. MPPA, as a GO, violated the Standard by not establishing facility ratings that were consistent with an associated facility ratings methodology because MPPA did not provide a documented facility ratings methodology for the 48th Street Peaking Station until April 20, 2009.	FAC-009-1	R1	Medium	Severe	Reliability*First* found that this violation posed a moderate risk and did not pose a serious or substantial risk to the bulk power system (BPS) because upon development and application of its facility ratings methodology, MPPA confirmed that it had correctly identified the most limiting element in its facility ratings in place during the time period of the alleged violation. In addition, there were no instances since June 18, 2007 of thermal overloads or exceeding of established ratings at the 48th Street Peaking Station.	June 18, 2007, the date MPPA registered with NERC Compliance Registry.	June 9, 2011, the date MPPA provided documentation of facility ratings for the 48th Street Peaking Station consistent with its facility ratings methodology.	$12,000 (for RFC200900219; RFC200900220; RFC200900221; and RFC200900222)	Compliance Audit	MPAA submitted its facility ratings methodology to Reliability*First* and later retained a technical consultant, and enhanced its facility ratings documentation by including more background information and descriptions to ensure that it was consistent with its facility ratings methodology.	6/9/2011	9/13/2011	Neither Admits nor Denies	Reliability*First* considered certain aspects of MPPA's compliance program as mitigating factors in the penalty determination. For example, MPPA's Compliance Manager and Senior Engineer meet with key member personnel on an annual basis. Additionally, MPPA holds workshops to advise both member and non-member cities on compliance issues. MPPA's compliance program has the support and involvement of senior management, including MPPA's General Manager. The Compliance Manager reports directly to the General Manager and the two are in regular and frequent contact. In addition, the Compliance Manager regularly attends meetings of the Board of Commissioners (MPPA's governing body) and reports on the compliance program as part of the regular agenda. MPPA's Compliance Policy requires ongoing internal auditing and monitoring of the implementation of its compliance program and MPPA has hired consultants to conduct audits. MPPA's General Manager has issued guidelines indicating that lack of compliance with the statutory and regulatory standards will affect employee compensation and opportunities for promotion.
Reliability*First* Corporation (RFC)	Midland Cogeneration Venture, Limited Partnership (Midland)	NCR10282	RFC201000673	Settlement Agreement	During a compliance audit from October 18, 2010 through October 29, 2010, Reliability*First* determined that Midland, as a Generator Operator, failed to maintain the generator schedule as directed by its Transmission Operator ("TOP"). Midland's TOP set the voltage schedule for the relevant time period for 360 kV for the hours between 0700 and 2300, with a tolerance band of plus or minus 2 kV. On April 7, 2010, Midland's voltage failed to reach 360 kV, and failed to stay within the specified tolerance band (358 kV to 362 kV) for most of the hours between 0700 and 2300 because 75% of its generators were offline. Midland's voltage remained at approximately 357 kV during those hours.	VAR-002-1	R2	Medium	Lower	Reliability*First* found that due to the nature of the violation, offset by the mitigating factors, this violation posed a moderate risk to the reliability of the bulk power system (BPS). This risk was mitigated by the fact that Midland's voltage never dropped below 357 kV, which is above the nominal voltage of 345 kV. Midland monitored the electrical parameters of its generators, including the voltage and current. In addition, Midland's control system has alarming capability, and the alarms sound when voltage is 362 kV and above or 353 kV and below. Thus, the alarms did not sound.	April 7, 2010, the date Midland failed to maintain its voltage schedule.	April 7, 2010.	$40,000 (for RFC201000610, RFC201000611, RFC201000673, and RFC201000755)	Compliance Audit	Midland worked with its TOP to put in place a voltage schedule that takes into account that Midland's generation operations. Midland's TOP implemented a revised temporary voltage schedule until it completes a study regarding Midland. Midland also provided its operators with mandatory communication requirements regarding reporting its inability to meet its voltage schedule. In addition, Midland trained its personnel regarding the voltage schedule and implemented internal auditing for compliance with VAR-002.	1/3/2011	2/16/2011	Neither Admits nor Denies	Reliability*First* considered as a mitigating factor that Midland self reported two of the violations in this Agreement; however, Reliability*First* also considered that it discovered two of the violations at a Compliance Audit and did not provide mitigating credit for those violations. Reliability*First* considered certain aspects of Midland's internal compliance program as a mitigating factor. Midland distributes its compliance program throughout the organization, and the individuals with responsibility for compliance have access to the Chief Executive Officer. The Vice President and the General Counsel & Corporate Secretary oversee all regulatory compliance activities, and Midland expects all employees to identify potential noncompliance. Compliance program staff attends regional and national reliability seminars. In addition, Midland utilizes contractors to develop and manage its compliance program as well as to conduct compliance-based training. In addition, as part of its ongoing effort to enhance its operations and compliance with Reliability Standards, Midland began replacing the gas turbine AVRs on each generating unit. The new AVRs will provide better voltage control and provide real time information to operators if any issues arise. While Midland was previously only able to observe the alarms on the former AVRs at the individual units, the new AVRs will also alarm directly to the central control room.
Reliability*First* Corporation (RFC)	Midland Cogeneration Venture, Limited Partnership (Midland)	NCR10283	RFC201000610	Settlement Agreement	On September 3, 2010, Midland self-reported VAR-002-1, R3 to Reliability*First* . Midland, as a Generator Operator, failed to notify its Transmission Operator ("TOP") of a status change on its generator Reactive Power resource, specifically the status of the Automatic Voltage Regulator (AVR) on its generating Unit 14. Upon learning of issues regarding voltage control, Midland discovered that the AVR hardware on its generating Unit 14 failed, and as a result, Unit 14 was operating in manual mode. Midland had not adequately trained its operators to recognize when the voltage regulator was operating in manual mode or to report generating unit status changes. Reliability*First* dismissed a potential violation on June 16, 2011 as Midland had not anticipated the status change of the AVR on its generating Unit 14.	VAR-002-1	R3	Medium	Severe	Reliability*First* found that due to the nature of the violation, offset by the mitigating factors, this violation posed a moderate risk to the reliability of the bulk power system (BPS). The risk was mitigated by the fact that this violation affected only one of Midland's 15 generators. Midland eventually notified its TOP of the AVR failure and replaced the failed AVR. Midland continuously monitors the electrical parameters of its generators, including the voltage and current, which initially alerted Midland to the voltage control problems on Unit 14. Midland's operators perform local AVR status checks every four hours during normal generator operations and make necessary voltage adjustments, including during the time period of the violation. During the violation, Midland maintained its voltage schedule. Furthermore, if necessary, Midland could have compensated for the loss of Unit 14 because other generators at Midland's facility were operational at the time of the violation.	June 4, 2010, the date the AVR at Unit 14 failed.	September 3, 2010, the date Midland notified its TOP of the status change.	$40,000 (for RFC201000610, RFC201000611, RFC201000673, and RFC201000755)	Self-Report	Midland notified its TOP of the outage and provided all necessary information and dates surrounding the AVR outage to the TOP. Midland trained its maintenance, engineering and operations personnel regarding AVR status and outage reporting requirements. Control room operators were given the NERC required AVR outage reporting requirements. Midland's operator logs now demonstrate that AVR status is confirmed every four hours. Training was completed to strengthen Midland's culture of compliance, including topics on the awareness and the purpose of NERC and Reliability Standards, at an all-employee meeting. In addition, Midland will conduct periodic internal audits as well as audits completed by contractors to ensure compliance with AVR requirements.	12/3/2010	2/18/2011	Neither Admits nor Denies	Reliability*First* considered as a mitigating factor that Midland self reported two of the violations in this Agreement; however, Reliability*First* also considered that it discovered two of the violations at a Compliance Audit and did not provide mitigating credit for those violations. Reliability*First* considered certain aspects of Midland's internal compliance program as a mitigating factor. Midland distributes its compliance program throughout the organization, and the individuals with responsibility for compliance have access to the Chief Executive Officer. The Vice President and the General Counsel & Corporate Secretary oversee all regulatory compliance activities, and Midland expects all employees to identify potential noncompliance. Compliance program staff attends regional and national reliability seminars. In addition, Midland utilizes contractors to develop and manage its compliance program as well as to conduct compliance-based training. In addition, as part of its ongoing effort to enhance its operations and compliance with Reliability Standards, Midland began replacing the gas turbine AVRs on each generating unit. The new AVRs will provide better voltage control and provide real time information to operators if any issues arise. While Midland was previously only able to observe the alarms on the former AVRs at the individual units, the new AVRs will also alarm directly to the central control room.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* Corporation (RFC)	Midland Cogeneration Venture, Limited Partnership (Midland)	NCR10284	RFC201000755	Settlement Agreement	During a compliance audit from October 18, 2010 through October 29, 2010, Reliability*First* determined that Midland, as a Generator Owner that owns a generation Protection System, had a deficient generation Protection System maintenance and testing program. In Midland's Protection System maintenance and testing program prior to August 30, 2010, Midland failed to include maintenance and testing intervals and their basis for all Protection System devices that affect the reliability of the bulk power system (BPS). Midland also failed to include a summary of maintenance and testing procedures. Midland's revised Protection System maintenance and testing program, dated August 30, 2010 (August 30, 2010 Program) failed to include maintenance and testing intervals and their basis for communications systems, voltage and current sensing devices, batteries, and DC control circuitry. Furthermore, the August 30, 2010 Program failed to include a summary of maintenance and testing procedures for communications systems, voltage and current sensing devices, batteries, and DC control circuitry. This violation implicated all of Midland's 1,284 generation Protection System devices.	PRC-005-1	R1	High	Severe	Reliability*First* found that due to the nature of the violation, offset by the mitigating factors, this violation posed a moderate risk to the reliability of the bulk power system (BPS). The risk was mitigated by the fact that despite a deficient Protection System maintenance and testing program, Midland only failed to test 5.8% of its Protection System devices. In addition, Midland has in place a backup Protection System for all protected generation equipment. In addition the Unit 1 generator and both of Midland's transmission/interconnection lines have redundant protection. All primary, backup and redundant Protection Systems alarm to the control room. Furthermore, Midland's facility has alarms in place to alert plant personnel of the failure of sensing devices and station batteries. These alarms did not sound during the time period of the violation. Midland also completed regular visual inspections on all Protection System devices.	December 9, 2008, the date Midland was required to comply with the Standard.	March 30, 2011, the date Midland revised its Protection System maintenance and testing program.	$40,000 (for RFC201000610, RFC201000611, RFC201000673, and RFC201000755)	Compliance Audit	Midland developed a revised Protection System maintenance and testing program that addressed the deficiencies of the August 30, 2010 Program. Additions included maintenance and testing intervals and their basis for communications systems, voltage and current sensing devices, batteries and DC control circuitry. Furthermore, a summary of maintenance and testing procedures for communications systems, voltage and current sensing devices, batteries and DC control circuitry was included in the revised document dated December 3, 2010. During the Reliability*First* review of the evidence of Mitigation Plan completion, Reliability*First* discovered that due to a misunderstanding of the Reliability*First* definition of the bulk power system (BPS), 16 relays were not included in Midland's document. Midland provided a revision of its Protection System device summary table for relays dated March 30, 2011, that included the 16 relays previously omitted. Even though these relays had not previously been included in Midland's formal Protection System maintenance and testing program, Reliability*First* reviewed the dates the 16 relays were last tested and maintained and found they were within the defined interval. Midland missed its original mitigation completion date due to this misunderstanding of the BPS definition.	3/30/2011	5/26/2011	Neither Admits nor Denies	Reliability*First* considered as a mitigating factor that Midland self-reported two of the violations in this Agreement; however, Reliability*First* also considered that it discovered two of the violations at a Compliance Audit and did not provide mitigating credit for those violations. Reliability*First* considered certain aspects of Midland's internal compliance program as a mitigating factor. Midland distributes its compliance program throughout the organization, and the individuals with responsibility for compliance have access to the Chief Executive Officer. The Vice President and the General Counsel & Corporate Secretary oversee all regulatory compliance activities, and Midland expects all employees to identify potential noncompliance. Compliance program staff attends regional and national reliability seminars. In addition, Midland utilizes contractors to develop and manage its compliance program as well as to conduct compliance-based training. In addition, as part of its ongoing effort to enhance its operations and compliance with Reliability Standards, Midland began replacing the gas turbine AVRs on each generating unit. The new AVRs will provide better voltage control and provide real time information to operators if any issues arise. While Midland was previously only able to observe the alarms on the former AVRs at the individual units, the new AVRs will also alarm directly to the central control room.
Reliability*First* Corporation (RFC)	Midland Cogeneration Venture, Limited Partnership (Midland)	NCR10285	RFC201000611	Settlement Agreement	On September 3, 2010, Midland self-reported PRC-005-1 R2 to Reliability*First* . Midland, as a Generator Owner that owns a generation Protection System, failed to have complete documentation regarding the maintenance and testing of a number of its protective relays. Specifically, Midland failed to provide evidence that it performed maintenance and testing on 75 of its 479 (15.7%) protective relays within their defined intervals, which constitutes 5.8% of its 1,284 generation Protection System devices. Furthermore, Midland failed to provide the date it last maintained and tested its protective relays.	PRC-005-1	R2	High	Lower	Reliability*First* found that due to the nature of the violation, offset by the mitigating factors, this violation posed a moderate risk to the reliability of the bulk power system (BPS). The risk was mitigated by the fact that although Midland provided no prior interval testing evidence, after Midland discovered the violation, it tested all Protection System devices and found them all to be functional; however, ten of the protective relays were out of calibration. These protective relays did not jeopardize any equipment because they were more sensitive to certain fault conditions. Due to the miscalibration of the protective relays, the zone of protection extended further from the Midland facility than designed, resulting in a reported Misoperation on February 12, 2009. Midland implemented a corrective action plan whereby it repaired and recalibrated the relay on March 31, 2009. Additionally, Midland has in place a backup Protection System for all protected generation equipment. In addition, the Unit I generator and both of Midland's transmission/interconnection lines have redundant protection as well. Furthermore, all primary, backup, and redundant Protection Systems alarm to the control room. Midland's facility has alarms in place to alert plant personnel of the failure of sensing devices and station batteries. These alarms did not sound throughout the duration of the violation. Furthermore, Midland's facility has alarms in place to alert plant personnel if sensing devices and station batteries failed. Midland also completed regular visual inspections of all generation Protection System devices.	December 9, 2008, the date Midland was required to comply with the Standard.	April 11, 2011, the date Midland completed testing of all relevant generation Protection System devices.	$40,000 (for RFC201000610, RFC201000611, RFC201000673, and RFC201000755)	Self-Report	Midland tested all 75 relay devices for which it lacked evidence of testing and provided the date last tested and maintained. 71 relays were last tested and maintained by February 27, 2010. Even though Midland's list of protection relays indicated the last date that the remaining four relays were tested/maintained and that the relays had returned to compliance by September 9, 2009, Midland could not locate the corresponding test records. Therefore, Midland tested the relays and provided documents to show that the maintenance and testing for four relays was performed on April 11, 2011. Midland also developed a revised Protection System maintenance and testing program to ensure clarity and compliance as explained in its Mitigation Plan actions for PRC-005-1 R1.	4/11/2011	4/12/2011	Neither Admits nor Denies	Reliability*First* considered as a mitigating factor that Midland self-reported two of the violations in this Agreement; however, Reliability*First* also considered that it discovered two of the violations at a Compliance Audit and did not provide mitigating credit for those violations. Reliability*First* considered certain aspects of Midland's internal compliance program as a mitigating factor. Midland distributes its compliance program throughout the organization, and the individuals with responsibility for compliance have access to the Chief Executive Officer. The Vice President and the General Counsel & Corporate Secretary oversee all regulatory compliance activities, and Midland expects all employees to identify potential noncompliance. Compliance program staff attends regional and national reliability seminars. In addition, Midland utilizes contractors to develop and manage its compliance program as well as to conduct compliance-based training. In addition, as part of its ongoing effort to enhance its operations and compliance with Reliability Standards, Midland began replacing the gas turbine AVRs on each generating unit. The new AVRs will provide better voltage control and provide real time information to operators if any issues arise. While Midland was previously only able to observe the alarms on the former AVRs at the individual units, the new AVRs will also alarm directly to the central control room.
Reliability*First* Corporation (RFC)	Morgantown Energy Associates (Morgantown)	NCR00834	RFC201000669	Settlement Agreement	On October 29, 2010, Morgantown self-certified its noncompliance with VAR-002-1 R1. Reliability*First* determined that Morgantown, as a Generator Operator (GOP), did not operate the automatic voltage regulator in automatic voltage control mode, as required by the Standard, instead operating the automatic voltage regulator in power factor mode as a normal mode of operations.	VAR-002-1	R1	Medium	Severe	Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because while the generator may not have been operating in automatic voltage mode, Morgantown was operating the generator in the automatic power factor control mode. In addition, Morgantown monitored its voltage and facility limits at all times. Furthermore, Morgantown has a single 138 kV connection to the BPS and is a minimal power productive entity of only 50 MW.	8/2/2007	9/6/2010	$15,000 (for RFC201000669, RFC201000670 and RFC201100781)	Self-Certification	Morgantown mitigated the issue by issuing standing orders to its operating personnel to notify its TOP of any changes in the operating status of its automatic voltage regulator and at any time it cannot maintain the TOP's prescribed voltage schedule. In addition, Morgantown trained its personnel on the new standing orders and generally on the Standard.	10/21/2010	3/9/2011	Neither Admits nor Denies	Reliability*First* considered Morgantown's internal compliance program (ICP) as a mitigating factor in assessing the penalty. Morgantown's ICP addresses NERC standards and requirements applicable to GOs and GOPs, describes how compliance with these requirements is met, and references external documents. The ICP is supplemented with a corporate reliability policy, an assessment program, and a group dedicated to compliance.
Reliability*First* Corporation (RFC)	Morgantown Energy Associates (Morgantown)	NCR00834	RFC201000670	Settlement Agreement	On October 29, 2010, Morgantown self-certified its noncompliance with VAR-002-1 R2. Reliability*First* determined that Morgantown, as a GOP, during periods of low system voltage, could not maintain the voltage schedule prescribed by its Transmission Operator as required by the Standard. Morgantown failed to contact its Transmission Operator (TOP) during these periods and was therefore not exempt from following the voltage schedule.	VAR-002-1	R2	Medium	Severe	Reliability*First* determined that the issue posed a minimal risk to the reliability of the bulk power system (BPS) because while the generator may not have been operating in automatic voltage mode, Morgantown was operating the generator in the automatic power factor control mode. In addition, Morgantown monitored its voltage and facility limits at all times. Furthermore, Morgantown has a single 138 kV connection to the BPS and is a minimal power productive entity of only 50 MW.	8/2/2007	9/6/2010	$15,000 (for RFC201000669, RFC201000670 and RFC201100781)	Self-Certification	Morgantown mitigated the issue by issuing standing orders to its operating personnel to notify its TOP of any changes in the operating status of its automatic voltage regulator and at any time it cannot maintain the TOP's prescribed voltage schedule. In addition, Morgantown trained its personnel on the new standing orders and generally on the Standard.	10/21/2010	3/9/2011	Neither Admits nor Denies	Reliability*First* considered Morgantown's ICP as a mitigating factor in assessing the penalty. Morgantown's ICP addresses NERC standards and requirements applicable to GOs and GOPs, describes how compliance with these requirements is met, and references external documents. The ICP is supplemented with a corporate reliability policy, an assessment program, and a group dedicated to compliance.
Reliability*First* Corporation (RFC)	Morgantown Energy Associates (Morgantown)	NCR00834	RFC201100781	Settlement Agreement	On February 28, 2011, Morgantown self-reported a violation of PRC-005-1 R1 and R2. Reliability*First* determined that Morgantown, as a Generator Owner, failed to document a Protection System maintenance and testing program for its batteries. Specifically, Morgantown failed to define maintenance and testing intervals and their basis for its batteries. This involved a total of four battery banks, less than one percent of Morgantown's 504 Protection System devices in 2007 and 2008. Reliability*First* determined that the facts implicated only PRC-005-1 R1 because Morgantown had documented implementation of its maintenance and testing program, pursuant to PRC-005-1 R2, but that program was deficient.	PRC-005-1	R1	High	Low	Reliability*First* determined that this violation did not pose a serious or substantial risk to the bulk power system (BPS) because Morgantown implemented redundant protections. Specifically, Morgantown's primary source of direct current power is two 100% capacity battery chargers, one of which in service with the other in automatic standby mode. Each battery charger is powered from different motor control centers, with each motor control center supplied by a different power source. The battery chargers and batteries are continuously monitored. Morgantown also conducted routine battery surveillance in 2006, as well as battery load test in August of 2006. Data is available beginning December 1, 2008 for routine battery surveillance with satisfactory results. Additionally, Morgantown tested other Protection System devices during the identified period of missing battery data and determined that no misoperations occurred during the missed testing interval period.	June 25, 2007(the date Qualifying Facilities were responsible to comply with the Reliability Standards)	11/14/2008	$15,000 (for RFC201000669, RFC201000670 and RFC201100781)	Self-Report	On April 1, 2011, Morgantown submitted a mitigation plan addressing this violation. In this mitigation plan, Morgantown memorialized the actions it took to mitigate this violation by enhancing Protection System program document with descriptions of battery maintenance specifications. In November of 2008, Morgantown began to follow its new program for battery testing and by November 14, 2008, Morgantown completed all relevant testing.	11/14/2008	6/9/2011	Neither Admits nor Denies	Reliability*First* considered Morgantown's ICP as a mitigating factor in assessing the penalty. Morgantown's ICP addresses NERC standards and requirements applicable to GOs and GOPs, describes how compliance with these requirements is met, and references external documents. The ICP is supplemented with a corporate reliability policy, an assessment program, and a group dedicated to compliance. In addition, Reliability*First* considered Morgantown's Self Report of the PRC-005-1 R1 to be a mitigating factor.
Reliability*First* Corporation (RFC)	Ohio Valley Electric Corporation (OVEC)	NCR00857	RFC201000301	Settlement Agreement	On March 30, 2010, OVEC, as a Generator Operator, submitted a Self-Report dated March 29, 2010 to Reliability*First* for a violation of VAR-002-1.1a R3. During a compliance audit from June 8, 2010 through June 11, 2010, Reliability*First* reviewed the Self-Report and concluded that OVEC failed to notify its Transmission Operator that it operated one of its generators in manual mode. In the Self-Report, OVEC stated that on October 18, 2009, OVEC's Clifty Creek Unit No. 6 generator (Unit No. 6) returned to service after being offline for a tube leak. The Automatic Voltage Regulator (AVR) was not in service at the time OVEC returned Unit No. 6 to service. Therefore OVEC operated Unit No. 6 in manual mode, rather than in automatic voltage control mode. OVEC did not notify the Transmission Operator of this occurrence until two hours and thirty minutes after OVEC operated Unit No. 6 in manual mode. Reliability*First* found that OVEC violated VAR-002-1.1a R1 by failing to notify the Transmission Operator of the operation of a generator connected to the interconnected transmission system in manual voltage control mode.	VAR-002-1.1a	R1	Medium	Lower	Reliability*First* determined that this violation posed a moderate risk but did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Unit No. 6 is located at a generating station which contains five other generators of similar capacity and vintage. The remaining five generators had their AVRs in service and were maintaining voltage during the period of the violation, which would compensate for any voltage variations during this period. Additionally, OVEC manually controlled the voltage on Unit No. 6, adhering to all issued voltage schedules during the time period of the violation.	10/18/2009	10/18/2009	$15,000 (for RFC201000301 and RFC201000320)	Self-Report	On September 21, 2010, OVEC submitted a Mitigation Plan to Reliability*First* addressing the violation of VAR-002-1.1a R1. In this plan, OVEC memorialized the actions it took to address the violation of VAR-002-1.1a R1. OVEC installed monitoring points to monitor the AVR status of its generators via the OVEC SCADA system. Monitoring points are now located on every AVR on each generator. The OVEC SCADA system alarms upon any change in AVR status, thus notifying the system operator immediately.	5/17/2010	11/23/2010	Admits	Reliability*First* considered OVEC's internal compliance program (ICP) as a mitigating factor in assessing the penalty.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Reliability*First* Corporation (RFC)	Ohio Valley Electric Corporation (OVEC)	NCR00857	RFC201000320	Settlement Agreement	On April 9, 2010, OVEC, as a Balancing Authority and Transmission Operator, self-reported to Reliability*First* a possible violation of COM-002-2 R2. OVEC identified an event that occurred on February 1, 2010, during which OVEC issued a directive regarding a switching operation to remove the 345 kV circuit breaker "F" at the Kyger Creek Substation. During this event, OVEC did not ensure that the recipient of the directive repeated the information back correctly. Reliability*First* found that OVEC violated COM-002-2 R2 by failing to ensure the recipient of the directive repeated the information back correctly.	COM-002-2	R2	Medium	High	Reliability*First* determined that this violation posed a moderate risk did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Prior to the occurrence of the violation, OVEC created procedures to ensure the appropriate issuance of directives, provided proper training to employees on the use of these procedures, and routinely reviewed recordings to verify that the procedures are followed. Therefore, OVEC had procedures in place for the use of three-part communications and this violation did not evidence a systemic problem, but rather, an isolated incident. Furthermore, the recipient of the directive completed the switching operation successfully, and the circuit breaker on which the switching was performed resides in a substation that contains six breaker bays. In the event that OVEC had taken one breaker out of service due to an unclear directive, the redundant bus ties and breaker bay configuration would have minimized the impact on the BPS.	2/1/2010	2/1/2010	$15,000 (for RFC201000301 and RFC201000320)	Self-Report	On May 19, 2010, OVEC submitted a Mitigation Plan to Reliability*First* addressing the violation of COM-002-2 R2. In this plan, OVEC memorialized the actions it took to address the violation of COM-002-2 R2. OVEC refreshed the training of all system operators and field switching personnel, to reinforce the principles and importance of three-part communications. OVEC also committed to providing refresher training on three-part communications on a periodic basis.	7/30/2010	8/12/2010	Admits	Reliability*First* considered OVEC's internal compliance program (ICP) as a mitigating factor in assessing the penalty.
Reliability*First* Corporation (RFC)	Panda Brandywine LP (Panda)	NCR00866	RFC201000640	Settlement Agreement	During a compliance audit of Panda from September 13, 2010 through September 28, 2010 (Audit), Reliability*First* determined that Panda, as a Generator Owner that owns a generation Protection System, did not include maintenance and testing intervals and their basis or a summary of maintenance and testing procedures for any of Panda's 15 DC control circuits in its Protection System maintenance and testing program (Program).	PRC-005-1	R1	High	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Panda visually inspected, on a daily basis, all DC control circuits that are not enclosed within other equipment, and identified no issues. (Approximately 40% of Panda's DC control circuits are not enclosed within other equipment.) Panda's daily visual inspections included an inspection of the lock-out relays associated with the DC control circuits. Additionally, Panda identified no issues upon the full testing of all the DC control circuits and determined that the DC control circuits were in excellent working order.	6/18/2007	11/23/2010	$50,000 (for RFC201000640, RFC201000641, RFC201000642, and RFC201000644)	Compliance Audit	On November 11, 2010, Panda submitted to Reliability*First* its mitigation plan to address the violation of PRC-005-1 R1. Panda amended its Program to include maintenance and testing intervals and their basis and a summary of maintenance and testing procedures for its DC control circuits. Panda also maintained and tested its DC control circuits.	11/23/2010	5/5/2011	Admits	Reliability*First* considered as a mitigating factor certain aspects of Panda's compliance program. For instance, Panda reviews and modifies its internal compliance program as necessary and performs assessments of compliance activities through the use of independent third parties specializing in NERC compliance. Panda's internal compliance program is supervised by Panda's General Manager, who also has direct access to the CEO of Panda's parent company, Panda Energy Corporation. Panda, its parent company Panda Energy Corporation, and its affiliated companies have no prior violations of the Reliability Standards. As a result, this violation does not constitute a repetitive infraction.
Reliability*First* Corporation (RFC)	Panda Brandywine LP (Panda)	NCR00866	RFC201000641	Settlement Agreement	During a compliance audit of Panda from September 13, 2010 through September 28, 2010, Reliability*First* determined that Panda, as a Generator Owner that owns a generation Protection System, could not provide evidence that it maintained and tested its voltage and current sensing devices within the defined intervals of its Protection System maintenance and testing program. Specifically, Panda failed to test any of its 149 voltage and current sensing devices since 1996, and therefore missed its seven-year maintenance and testing intervals for voltage and current sensing devices. Panda represents that it misinterpreted PRC-005-1 R2.1's requirement to maintain and test its voltage and current sensing devices within defined intervals. Specifically, Panda believed that the calculation of the defined intervals for its voltage and current sensing devices began on the first day of mandatory compliance. As a result of this misinterpretation, Panda believed it was required to maintain and test its voltage and current sensing devices any time prior to June 18, 2014.	PRC-005-1	R2.1	High	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Panda visually inspected, on a daily basis, all voltage sensing devices that are not enclosed within other equipment, and verified that those voltage sensing devices were in excellent working condition. Approximately 50% of Panda's voltage sensing devices are not enclosed within other equipment. Panda's current sensing devices are enclosed in circuit breaker bushings or other equipment, which prevents daily visual inspection. Panda's voltage sensing devices have alarms that alert Panda to any abnormal conditions, and these alarms did not sound during the time period of the violation. Additionally, Panda identified no issues upon testing all voltage and current sensing devices in November 2010, and confirmed that all voltage and current sensing devices were in excellent working condition.	6/18/2007	11/19/2010	$50,000 (for RFC201000640, RFC201000641, RFC201000642, and RFC201000644)	Compliance Audit	On November 11, 2010, Panda submitted to Reliability*First* its mitigation plan to address the violation of PRC-005-1 R2.1. Panda maintained and tested its voltage and current sensing devices. In addition, Panda developed a document that will reference and track the maintenance and testing of voltage and current sensing devices.	11/19/2010	5/6/2011	Admits	Reliability*First* considered as a mitigating factor certain aspects of Panda's compliance program. For instance, Panda reviews and modifies its internal compliance program as necessary and performs assessments of compliance activities through the use of independent third parties specializing in NERC compliance. Panda's internal compliance program is supervised by Panda's General Manager, who also has direct access to the CEO of Panda's parent company, Panda Energy Corporation. Panda, its parent company Panda Energy Corporation, and its affiliated companies have no prior violations of the Reliability Standards. As a result, this violation does not constitute a repetitive infraction.
Reliability*First* Corporation (RFC)	Panda Brandywine LP (Panda)	NCR00866	RFC201000642	Settlement Agreement	During a compliance audit of Panda from September 13, 2010 through September 28, 2010, Reliability*First* discovered a violation of PRC-001-1 R1. Panda, as a Generator Operator (GOP), failed to provide sufficient evidence to demonstrate that operations personnel were familiar with the purpose and limitations of protection system schemes applied in Panda's area.	PRC-001-1	R1	High	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Panda's training program did train its operations personnel on the fundamental aspects of electrical components, switching, and electrical systems, including the fundamental aspects of relay protection systems. Panda represents that it provided information to its operations personnel on the relay protection system schemes specific to the Panda facility *via* on the job training.	2/25/2008 (GOP registration date)	12/15/2010	$50,000 (for RFC201000640, RFC201000641, RFC201000642, and RFC201000644)	Compliance Audit	On November 11, 2010, Panda submitted to Reliability*First* its mitigation plan to address the violation of PRC-001-1 R1. Panda amended its training program for operations personnel to include information on the relay protection system schemes specific to the Panda facility. Panda documented and maintained records for all employees who successfully completed the training program.	12/15/2010	5/6/2011	Admits	Reliability*First* considered as a mitigating factor certain aspects of Panda's compliance program. For instance, Panda reviews and modifies its internal compliance program as necessary and performs assessments of compliance activities through the use of independent third parties specializing in NERC compliance. Panda's internal compliance program is supervised by Panda's General Manager, who also has direct access to the CEO of Panda's parent company, Panda Energy Corporation. Panda, its parent company Panda Energy Corporation, and its affiliated companies have no prior violations of the Reliability Standards. As a result, this violation does not constitute a repetitive infraction.
Reliability*First* Corporation (RFC)	Panda Brandywine LP (Panda)	NCR00866	RFC201000644	Settlement Agreement	During a compliance audit of Panda from September 13, 2010 through September 28, 2010, Reliability*First* determined that Panda, as a Generator Operator (GOP), failed to maintain its voltage within its Transmission Operator's voltage schedule. PJM Interconnection, LLC (PJM) is Panda's Transmission Operator. *PJM Manual 03*, which was publicly posted on the PJM website, provided a default voltage schedule of 235 with a bandwidth of +/- 4.0, which governed Panda. Although, Panda was required to follow this default voltage schedule, Panda operated outside PJM's voltage schedule without first receiving an exemption on several occasions. Specifically, Panda exceeded the high limit of 239 kV of the default voltage schedule on July 15, 2010, July 21, 2010, August 5, 2010 and August 31, 2010. On July 15, 2010, Panda operated at approximately 240 kV for one hour and forty eight minutes. On July 21, 2010, Panda operated between 241 kV and 240 kV for approximately two hours and thirty minutes. On August 5, 2010, Panda operated slightly above 239 kV for approximately twenty four minutes. On August 13, 2010, Panda operated between 239 kV and 241 kV for approximately one hour.	VAR-002-1.1a	R2	Medium	Severe	Reliability*First* determined that this violation posed a moderate risk but did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Panda operated in accordance with a power purchase agreement and Interconnection agreement with its Transmission Owner, which required Panda to maintain a nominal voltage of 230 kV, with reasonable variation of frequency and voltage consistent with prudent utility practices. Panda worked with its Transmission Owner and received a custom voltage schedule with an increased bandwidth that was consistent with Panda's historical operating practices. The Automatic Voltage Regulators at the Panda facility were in automatic mode at all times, and Panda continuously monitored voltage, amps, frequency, and real and Reactive Power at the Panda facility.	2/25/2008 (GOP registration date)	12/15/2010	$50,000 (for RFC201000640, RFC201000641, RFC201000642, and RFC201000644)	Compliance Audit	On January 26, 2011, Panda submitted to Reliability*First* its mitigation plan to address the violation of VAR-002-1.1a R1. In this mitigation plan, Panda validated the accuracy of its voltage readings, and set up automated alarming to ensure that its voltage does not exceed scheduled limits. Additionally, Panda received a custom voltage schedule from the Transmission Owner and began operating in accordance with that voltage schedule.	12/15/2010	4/14/2011	Admits	Reliability*First* considered as a mitigating factor certain aspects of Panda's compliance program. For instance, Panda reviews and modifies its internal compliance program as necessary and performs assessments of compliance activities through the use of independent third parties specializing in NERC compliance. Panda's internal compliance program is supervised by Panda's General Manager, who also has direct access to the CEO of Panda's parent company, Panda Energy Corporation. Panda, its parent company Panda Energy Corporation, and its affiliated companies have no prior violations of the Reliability Standards. As a result, this violation does not constitute a repetitive infraction.
Reliability*First* Corporation (RFC)	Troy Energy LLC (Troy Energy)	NCR00337	RFC201100723	Settlement Agreement	On January 7, 2011, Troy Energy, as a Generator Owner ("GO"), submitted a self-report to Reliability*First* identifying a possible violation of PRC-005-1, R2.1. Troy Energy reported that it failed to perform monthly battery maintenance and testing program ("Program") for the month of December, 2010, and that it failed to perform quarterly battery maintenance within the defined intervals of its Program for the fourth quarter of 2010. Specifically, on December 29, 2010, Troy Energy's general counsel received a letter from a Troy Energy employee alleging a possible violation of PRC-005-1 at the Troy Energy facility. In the letter, the Troy Energy employee alleged that the monthly and quarterly battery maintenance records at the Troy Energy facility were inaccurate and battery maintenance occurred outside the defined intervals of Troy Energy's Program. Troy Energy immediately initiated an internal investigation into the allegations, reviewed its records, interviewed all employees and examined its computer systems. Upon its completion of the internal investigation on January 5, 2011, Troy Energy concluded that, consistent with the employee's allegations, Troy Energy did not perform its December 2010 monthly battery maintenance until January 3, 2011. Troy Energy came to this conclusion even though its records stated that this monthly battery maintenance had occurred on December 14, 2010. Troy Energy also concluded that it failed to perform quarterly battery maintenance for the fourth quarter of 2010.	PRC-005-1	R2.1	High	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system ("BPS"). The risk to the reliability of the BPS was reduced, impart due to the duration. Troy Energy missed its monthly and quarterly battery maintenance intervals by only three and six days, respectively. Additionally, Troy Energy has alarms associated with its batteries to notify its operators of ground faults, low voltage, or charger problems. These alarms did not sound during the time period of the violation. Troy Energy's facility was not called into service and its generators did not operate during the time period of the alleged violation. Troy Energy's subsequent late battery maintenance did not reveal any abnormal conditions.	January 1, 2011, the date by which Troy Energy should have completed its monthly and quarterly battery maintenance.	January 6, 2011, the date Troy Energy completed its quarterly battery maintenance.	$10,000 (for RFC201100723)	Self-Report	Troy Energy conducted all deficient monthly and quarterly battery maintenance on January 3, 2011 and January 6, 2011, respectively. As a disciplinary action, Troy Energy removed the plant manager who was responsible during the time period of the alleged violation from his position as well as the responsible employee. The President of International Power America, Inc. was personally involved in the decision to remove the plant manager and the responsible employee from their duties. Additionally, Troy Energy now requires the Director of Compliance to personally review the evidence of completion for all Reliability Standard related tasks, including battery maintenance records, on the 21st day of each month. Troy Energy also conducted additional training emphasizing the importance of the Reliability Standards and the need to perform all required maintenance within the defined intervals of its Program.	1/18/2011	5/12/2011	Agrees and Stipulates	Reliability*First* considered certain aspects of Troy Energy's compliance program as mitigating factors. For instance, Troy Energy reviews all internal compliance procedures and practices annually. Troy Energy's Director of Corporate Services has direct access to the CEO of International Power America, Inc. International Power America, Inc. serves Troy Energy as a professional resource for internal assessment program modeling which include compliance driven audits and spot checks. When assessing the penalty for the alleged violation at issue, Reliability*First* considered Troy Energy's violation history. Troy Energy has a prior violation of PRC-005-1, R2.1. Additionally, Troy Energy's affiliate company, Armstrong Energy Limited Partnership, LLLP, (Armstrong Energy) has a violation of PRC-005-1, R1. As a result of these findings, Reliability*First* considered the violation as a repetitive infraction and the infraction an aggravating factor.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900131	Settlement Agreement	During an August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE determined that Lubbock, as a Transmission Owner (TO), did not have documentation of facility connection requirements for prospective generation, transmission, and end user facilities.	FAC-001-0	R1, R1.1, R1.2, R1.3	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock is a full requirements customer of the Southwestern Public Service Company (SPS). Lubbock's full requirements contract with SPS includes contractual obligations that would cause Lubbock to fully vet any proposed connection to its 230 kV system with SPS. Additionally, the function and physical make-up of Lubbock's 230 kV facilities limits the potential for any possible interconnections. Lubbock owns only 8.45 miles of 230 kV transmission lines which only function to connect Lubbock's 69 kV system to the 230 kV system of SPS.	1/30/2009 (the date Lubbock registered as a TO)	10/27/2010 (Mitigation Plan completion)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Compliance Audit	Lubbock has created, maintained and published a facility connection requirements document and has made this document available to the users of the transmission system, the Regional Reliability Organization and NERC. This document addressed Reliability Standard FAC-001-0 R1-R3 and all required sub-requirements.	10/27/2010	11/15/2010	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900132	Settlement Agreement	During an August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE determined that Lubbock, as a Transmission Owner (TO), did not have documentation of facility connection requirements for prospective generation, transmission, and end user facilities and could not provide a written summary of its plans to achieve the required system performance as described above throughout the planning horizon.	FAC-001-0	R2, R2.1 et seq.	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock is a full requirements customer of the Southwestern Public Service Company (SPS). Lubbock's full requirements contract with SPS includes contractual obligations that would cause Lubbock to fully vet any proposed connection to its 230 kV system with SPS. Additionally, the function and physical make-up of Lubbock's 230 kV facilities limits the potential for any possible interconnections. Lubbock owns only 8.45 miles of 230 kV transmission lines which only function to connect Lubbock's 69 kV system to the 230 kV system of SPS.	1/30/2009 (the date Lubbock registered as a TO)	10/27/2010 (Mitigation Plan completion)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Compliance Audit	Lubbock has created, maintained and published a facility connection requirements document and has made this document available to the users of the transmission system, the Regional Reliability Organization and NERC. This document addressed Reliability Standard FAC-001-0 R1-R3 and all required sub-requirements.	10/27/2010	11/15/2010	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900133	Settlement Agreement	During an August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE determined that Lubbock, as a Transmission Owner (TO), did not provide documentation of facility connection requirements for prospective generation, transmission, and end user facilities and therefore did not maintain and update its facility connection requirements as required. Lubbock also did not make documentation of these requirements available to the users of the transmission system, the Regional Reliability Organization, and North American Electric Reliability Corporation (NERC) on request, within the five business days stated in the Standard.	FAC-001-0	R3	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock is a full requirements customer of the Southwestern Public Service Company (SPS). Lubbock's full requirements contract with SPS includes contractual obligations that would cause Lubbock to fully vet any proposed connection to its 230 kV system with SPS. Additionally, the function and physical make-up of Lubbock's 230 kV facilities limits the potential for any possible interconnections. Lubbock owns only 8.45 miles of 230 kV transmission lines which only function to connect Lubbock's 69 kV system to the 230 kV system of SPS.	1/30/2009 (the date Lubbock registered as a TO)	10/27/2010 (Mitigation Plan completion)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Compliance Audit	Lubbock has created, maintained and published a facility connection requirements document and has made this document available to the users of the transmission system, the Regional Reliability Organization and NERC. This document addressed Reliability Standard FAC-001-0 R1-R3 and all required sub-requirements.	10/27/2010	11/15/2010	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900081	Settlement Agreement	On June 17, 2009, Lubbock, as a Transmission Owner (TO) and Distribution Provider (DP) that owns a transmission Protection System, submitted a Self-Report to SPP RE stating that its transmission Protection System maintenance and testing program did not include current and potential transformers. Subsequently, in its August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE found that Lubbock's Protection System maintenance and testing program also failed to include maintenance and testing procedures for associated communication systems, current and potential transformers, and DC control circuitry. Additionally, while Lubbock's procedure outlined monthly inspections of its station batteries, the procedure did not include sufficient battery testing procedures. SPP RE subsequently determined that Lubbock did not own any associated communication systems and functionally tests its DC control circuitry as part of its 230 kV breaker inspection procedure. Therefore, Lubbock's failure to satisfy PRC-005-1 R1 (1.1, 1.2) is limited to Lubbock's 48 instrument transformers, and four 230 kV station battery banks. The battery banks and instrument transformers combined comprise 71% of Lubbock's total Protection System devices.	PRC-005-1	R1, R1.1, R1.2	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock's instrument transformers were initially tested when placed into service, and the outputs from these instrument transformers are constantly monitored by Lubbock's Supervisory Control and Data Acquisition (SCADA) system. Additionally, Lubbock was inspecting its station battery banks on a monthly basis. These tests included visual inspections and recording of the battery voltage.	8/24/2007 (the date Lubbock registered as a DP (Lubbock's TO registration was effective 1/30/2009))	1/18/2011 (Mitigation Plan completion)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Self-Report	Lubbock revised its substation maintenance procedures to include a summary of maintenance and testing procedures and intervals for its instrument transformers. Additionally, Lubbock amended its procedure to reflect that it does not own any associated communication systems. Finally, Lubbock amended its documentation to include a more extensive battery voltage test and monitoring procedure. This new procedure included disconnecting the battery charger and conducting six interval readings of voltage over a 30-minute timeframe.	1/18/2011	1/25/2011	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place. The Self-Report was made at the suggestion of SPP RE following an event analysis of an August 16, 2008 reportable event. As a result, no self-report credit was awarded.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900082	Settlement Agreement	On June 17, 2009, Lubbock, as a Transmission Owner (TO) and Distribution Provider (DP) that owns a transmission Protection System, submitted a Self-Report to SPP RE stating that its transmission Protection System maintenance and testing program did not include current and potential transformers. Subsequently, during an August 10, 2009 through August 11, 2009, on-site compliance audit, SPP RE also found that Lubbock could not provide evidence of testing for its associated communication systems, instrument transformers, and DC control circuitry. Additionally, while it could demonstrate monthly battery inspections, Lubbock could not provide documentation of adequate battery testing. SPP RE subsequently determined that Lubbock's Protection System maintenance and testing program did include the recorded dates of its breaker trip tests for its DC control circuitry. Additionally, because Lubbock does not own any associated communication systems, no test data was required. Therefore, this violation was limited to its 48 instrument transformers and four 230 kV station batteries.	PRC-005-1	R2, R2.1, R2.2	High	High	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock's instrument transformers were initially tested when placed into service and the outputs from these instrument transformers are constantly monitored by Lubbock's Supervisory Control and Data Acquisition (SCADA) system. Additionally, Lubbock was inspecting its station battery banks on a monthly basis. These tests included visual inspections and recording of the battery voltage.	8/24/2007 (the date Lubbock registered as a DP (Lubbock's TO registration was effective 1/30/2009))	12/30/2010 (Mitigation Plan completion)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Self-Report	Lubbock implemented its Protection System maintenance and testing plan and provided testing/maintenance records and the last testing/maintenance dates of its potential and current transformers. The maintenance and testing activities included current and voltage readings, visual inspections, connection checks and ratio verification. Additionally, Lubbock provided evidence of its annual station battery testing, which included periodic voltage checks occurring in six intervals over a time period of 30 minutes.	12/30/2010	1/19/2011	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place. The Self-Report was made at the suggestion of SPP RE following an event analysis of an August 16, 2008 reportable event. As a result, no self-report credit was awarded.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900084	Settlement Agreement	On June 17, 2009, Lubbock, as a Load Serving Entity, submitted a Self-Report to SPP RE indicating that on August 16, 2008, it experienced a reportable incident and in response submitted a twenty-four hour emergency alert to its Regional Reliability Organization, the North American Electric Reliability Corporation (NERC), and the Department of Energy (DOE). Lubbock stated that it submitted the alert to NERC and DOE on an outdated form, and notified the wrong party at its Regional Reliability Organization. On August 10, 2009 through August 11, 2009, SPP RE conducted an on-site compliance audit of Lubbock and confirmed the statements made in Lubbock's Self-Report. Additionally, SPP RE determined that Lubbock submitted a subsequent alert report on August 20, 2008, utilizing the correct form. This form was submitted to NERC, DOE, and the appropriate contact at SPP RE.	EOP-004-1	R3, R3.1, R3.2	Lower	Severe	The violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because Lubbock did provide timely notification of the event to DOE and NERC, albeit on a prior version of the required form. Additionally, Lubbock had fully satisfied all of the reporting requirements as of August 20, 2008. Finally, Lubbock's Protection Systems operated properly to isolate the disturbance from the BPS. Therefore, the incident that Lubbock failed to report presented only minimal risk to the surrounding BPS.	8/16/2008 (the date the disturbance event occurred and the report was required to be submitted)	8/20/2008 (the date Lubbock sent the correct form and notified the correct parties)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Self-Report	Lubbock has implemented a documented procedure to ensure the proper disturbance reporting of DOE reportable incidents in the future. Within that procedure it has attached the appropriate reporting form, and it has specifically identified the appropriate contact at its Regional Reliability Organization, NERC, and DOE.	12/30/2010	1/12/2011	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place. The Self-Report was made at the suggestion of SPP RE following an event analysis of an August 16, 2008 reportable event. As a result, no self-report credit was awarded.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP200900134	Settlement Agreement	During an August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE determined that Lubbock, as a Transmission Owner (TO), did not include a clear process for the immediate reporting of vegetation conditions that present an imminent threat of a transmission line outage in its transmission vegetation management program (TVMP). The full extent of Lubbock's process for reporting immediate vegetation threats was a statement indicating "[r]eport all vegetation related outages as soon as possible."	FAC-003-1	R1, R1.5	High	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because Lubbock's system is confined to the geographic area of the city of Lubbock, Texas. Within its transmission system, Lubbock has only approximately nine miles of 230 kV lines. These lines are foot patrolled annually, and any problems are required to be immediately reported. Lubbock's rights-of-way maintenance is conducted by Asplundh, Lubbock's vegetation management contractor. According to Lubbock, Asplundh is in daily contact with personnel at Lubbock while coordinating vegetation clearance activities, thereby reducing the risk that an imminent contact might not be reported during rights-of-way activities. Furthermore, the geographic proximity of the Lubbock system to its centralized control center in the city of Lubbock decreases the likelihood that an imminent outage threat would not reach the appropriate individuals.	1/30/2009 (the date Lubbock registered as a TO)	10/27/2010 (the date Lubbock completed its mitigation plan)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Compliance Audit	Lubbock has included, within its TVMP document, an instruction directing the immediate communication of vegetation conditions presenting an imminent threat to its transmission facilities to its control room dispatcher. The procedure lists contact numbers for the Lubbock dispatcher and the vegetation management contractor.	10/27/2010	11/5/2010	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place.
Southwest Power Pool Regional Entity (SPP RE)	Lubbock Power And Light (Lubbock)	NCR06048	SPP201100529	Settlement Agreement	During an August 10, 2009 through August 11, 2009 on-site compliance audit, SPP RE determined that Lubbock, as a Load Serving Entity (LSE), did not have a documented sabotage reporting procedure prior to August 18, 2008. On August 18, 2008, Lubbock approved a CIP-001 sabotage recognition and reporting procedure. This document outlined methods for identifying physical and cyber sabotage and processes for contacting operational personnel following a sabotage event. Accordingly, the SPP RE audit team found a violation of CIP-001-1 R1 from August 24, 2007, the date Lubbock registered as a LSE, until August 18, 2008, the date Lubbock implemented its sabotage recognition and reporting procedure.	CIP-001-1	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS) because despite Lubbock's failure to initially have a procedure for the identification and awareness of sabotage events, it had previously implemented an employee emergency action plan on March 1, 2006. This plan outlined the use of a public address system and notification of the most senior supervisor available in the event of an explosion, fire, workplace violence, power failure or bomb threat. Additionally, on November 30, 2007, Lubbock's dispatch personnel underwent sabotage training. This training included topics of both physical and cyber sabotage and outlined how those topics relate to critical infrastructure protection. Lubbock also included event reporting contacts at the North American Electric Reliability Corporation (NERC) and the Department of Homeland Security (DHS) in the training materials.	8/24/2007 (the date Lubbock registered as a LSE)	8/18/2008 (the date Lubbock implemented its sabotage reporting procedure)	$14,000 (for SPP200900131, SPP200900132, SPP200900133, SPP200900081, SPP200900082, SPP200900084, SPP200900134, and SPP201100529)	Compliance Audit	Lubbock implemented a formal procedure for the recognition and reporting of sabotage events in accordance with Reliability Standard CIP-001-1 R1. The procedure describes the process for identifying sabotage events and the process for contacting appropriate parties in response to an event.	8/18/2008	5/18/2011	Neither Admits nor Denies	While Lubbock did not have a documented compliance program at the time of the violation, the entity confirmed that it is working to put one in place.
Western Electricity Coordinating Council (WECC)	Electrical District No. 2 (ED2)	NCR05142	WECC201002329	Settlement Agreement	On December 15, 2010, WECC conducted an off-site compliance audit of ED2 and discovered a violation of CIP-001-1 R1. ED2, as a Load-Serving Entity (LSE), failed to have procedures for the recognition of sabotage events or procedures to make its staff aware of sabotage events.	CIP-001-1	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because ED2 has only a radial connection to a 115 kV transmission system. ED2 is a small entity covering a service area of approximately 100 square miles and a peak load of only 60 MW.	6/18/2007 (when the Standard became mandatory and enforceable)	4/1/2008 (when ED2 completed its sabotage response guidelines and procedures)	$6,500 (for WECC201002329, WECC201002330, WECC201002331, and WECC201002332)	Compliance Audit	ED2 completed its sabotage response guidelines and procedures - *Operating Procedure for Recognition, Response and Reporting of Sabotage Events.*	4/1/2008	8/4/2011	Agrees and stipulates to the facts	ED2 had mitigated this violation by April 1, 2008, before the December 15, 2010 Audit.
Western Electricity Coordinating Council (WECC)	Electrical District No. 2 (ED2)	NCR05142	WECC201002330	Settlement Agreement	On December 15, 2010, WECC conducted an off-site compliance audit of ED2 and discovered a violation of CIP-001-1 R2. ED2, as a LSE, failed to have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	CIP-001-1	R2	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because ED2 has only a radial connection to a 115 kV transmission system. ED2 is a small entity covering a service area of approximately 100 square miles and a peak load of only 60 MW.	6/18/2007 (when the Standard became mandatory and enforceable)	4/1/2008 (when ED2 completed its sabotage response guidelines and procedures)	$6,500 (for WECC201002329, WECC201002330, WECC201002331, and WECC201002332)	Compliance Audit	ED2 completed its sabotage response guidelines and procedures - *Operating Procedure for Recognition, Response and Reporting of Sabotage Events.*	4/1/2008	8/4/2011	Agrees and stipulates to the facts	ED2 had mitigated this violation by April 1, 2008, before the December 15, 2010 Audit.
Western Electricity Coordinating Council (WECC)	Electrical District No. 2 (ED2)	NCR05142	WECC201002331	Settlement Agreement	On December 15, 2010, WECC conducted an off-site compliance audit of ED2 and discovered a violation of CIP-001-1 R3. ED2, as a LSE, failed to provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	CIP-001-1	R3	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because ED2 has only a radial connection to a 115 kV transmission system. ED2 is a small entity covering a service area of approximately 100 square miles and a peak load of only 60 MW.	6/18/2007 (when the Standard became mandatory and enforceable)	4/1/2008 (when ED2 completed its sabotage response guidelines and procedures)	$6,500 (for WECC201002329, WECC201002330, WECC201002331, and WECC201002332)	Compliance Audit	ED2 completed its sabotage response guidelines and procedures - *Operating Procedure for Recognition, Response and Reporting of Sabotage Events.*	4/1/2008	8/4/2011	Agrees and stipulates to the facts	ED2 had mitigated this violation by April 1, 2008, before the December 15, 2010 Audit.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Western Electricity Coordinating Council (WECC)	Electrical District No. 2 (ED2)	NCR05142	WECC201002332	Settlement Agreement	On December 15, 2010, WECC conducted an off-site compliance audit of ED2 and discovered a violation of CIP-001-1 R4. ED2, as a LSE, failed to have communication contacts at its local FBI office.	CIP-001-1	R4	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because ED2 has only a radial connection to a 115 kV transmission system. ED2 is a small entity covering a service area of approximately 100 square miles and a peak load of only 60 MW.	6/18/2007 (when the Standard became mandatory and enforceable)	4/1/2008 (when ED2 established communication contacts with its local FBI office)	$6,500 (for WECC201002329, WECC201002330, WECC201002331, and WECC201002332)	Compliance Audit	ED2 established communication contacts with its local FBI office.	4/1/2008	8/4/2011	Agrees and stipulates to the facts	ED2 had mitigated this violation by April 1, 2008, before the December 15, 2010 Audit.
Western Electricity Coordinating Council (WECC)	Holy Cross Energy (HCE)	NCR05190	WECC201102420	Settlement Agreement	On June 10, 2010, HCE requested verification from Xcel Energy Inc. (Xcel), the company HCE contracted with to be responsible for Protection System operation and maintenance of HCE's facilities, that the four relays sets at the HCE-owned Wolcott and Cooley Mesa substations were in compliance with PRC-023-1. Verification of compliance was given by Xcel on June 30, 2010. On December 7, 2010, Xcel discovered that two distance relays (one relay set) at the Cooley Mesa Substation on line 5787 were not within range of the loadability standards prescribed under R1.1. Xcel implemented new relay settings consistent with the Standard on December 20, 2010 and reported noncompliance of PRC-023 to HCE in mid-January 2011. HCE thereafter conducted its own investigation to determine whether a reportable possible violation of PRC-023-1 existed. On November 1, 2010, WECC notified HCE that WECC was initiating the Self-Certification process for the period from January 1, 2010 to December 31, 2010. Under this process, HCE's Self-Certification submittal was due by February 16, 2011. On February 7, 2011, HCE submitted a Self-Report to WECC, during the Self-Certification submittal period, stating that the backup distance relay (Pkg-S) and the primary distance relay (Pkg-P) at its Cooley Mesa substation were not set in conformance with PRC-023-1 R1.1.	PRC-023-1	R1	High	Moderate	WECC determined that this violation posed a minimal risk to the reliability of the bulk power system (BPS). The scope of the violation includes two HCE relays located on a 230 kV transmission line that were set below the 150 percent threshold prescribed under PRC-023 R1.1. The risk posed by noncompliance is limited in that the relays were part of an extended zone of protection seldom called upon to operate. Further, the scope of the violation was limited to two relays on a single transmission line for a period less than six months. Finally, HCE is a single transmission facility operated by a third-party.	7/1/2010 (enforceable date of the Standard)	12/20/2010 (Mitigation Plan completion)	$5,000	Self-Report	On February 14, 2011, HCE submitted a completed Mitigation Plan indicating that HCE and Xcel, embarked on the following mitigation actions: 1) On December 9, 2010 the proper setting for relays was issued for Pkg-S and Pkg-P; 2) On December 20, 2010, relay settings were implemented and noncompliance was mitigated; and 3) HCE now requires Xcel to submit regular reports confirming ongoing PRC-023-1 compliance for all relays.	12/20/2010	4/5/2011	Admits to the Stipulated Facts in the Settlement Agreement	WECC did not consider an internal compliance program when assessing penalty.
Western Electricity Coordinating Council (WECC)	NAES Corporation - Burney	NCR05264	WECC201002403	Settlement Agreement	On December 30, 2010, NAES, as a Generator Operator, submitted a Self-Report addressing violations of VAR-002-1 R1 and R2, stating that due to a misunderstanding of its generator's configuration, NAES continuously operated its generator in power factor control mode during normal operations. NAES failed to notify the Transmission Operator that it was not operating in voltage control mode. WECC reviewed the Self-Report and determined that NAES operated its generator in a power factor mode instead of automatic voltage control mode and failed to notify its Transmission Operator of its operating mode, in violation of VAR-002-1 R1. Because NAES operated in a factor power mode from the start of mandatory compliance until January 4, 2011, WECC determined that there was no status or capability change on any of NAES's Reactive Power resources that may warrant an investigation of R3.	VAR-002-1	R1	Medium	Severe	This violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) and posed a minimal risk to the BPS because NAES maintained stable output of the unit despite not having an Automatic Voltage Regulator (AVR) in service. In addition, the risk was further mitigated by the fact that this violation is applicable to a single 30 MW generation facility with limited to minimal capacity to boost system voltage during BPS disturbances. The generator involved in this violation represents a small fraction of the total generation available to the Transmission Operator. For this reason, WECC determined that any potential harm would also be minimal, assuming a complete failure did not happen concurrent with protection system (even an N-1) failure. Also, NAES operated in power factor mode in accordance with the generator's capability curve.	8/2/2007 (when the Standard was enforceable and mandatory)	1/4/2011	$3,500 (for WECC201002403 and WECC201002404)	Self-Report	On February 2, 2011, NAES submitted a Mitigation Plan. On January 4, 2011, NAES notified its Transmission Operator that it operated in power factor mode, revised its plant procedures and trained its operators regarding the NAES AVR. NAES developed an operator log to track potential AVR issues associated with communication with NAES's Transmission Operator.	1/4/2011	4/5/2011	Agrees and Stipulates to the Facts in the Settlement Agreement.	Mitigating Factors: NAES's internal compliance program is well-documented and supported by corporate management, NAES has a budget for compliance activities, it empowers its employees to report noncompliance to management, and NAES may elect to take disciplinary actions against employees involved in violations of the Reliability Standards. WECC did not consider two prior violations of VAR-002-1 R1 by NAES's affiliates--NAES Corporation - Lincoln Generating Facility (NOC-476) and NAES Corporation - Covert (NOC-808)--to be aggravating factors in determining the penalty amount because there was not a commonality of compliance responsibility among the NAES affiliates.
Western Electricity Coordinating Council (WECC)	NAES Corporation - Burney	NCR05264	WECC201002404	Settlement Agreement	On December 30, 2010, NAES, as a Generator Operator, self-reported that it had received a voltage schedule in 2011 from its Transmission Operator. The voltage schedule was initially approved by the Transmission Operator in October 2008, and distributed to NAES in December 2008. However, NAES did not have the December 2008 schedule on file and did not maintain historical data on voltage levels and could not verify voltage levels. WECC determined that NAES's Transmission Operator provided NAES with a voltage schedule but NAES did not maintain its generator voltage or Reactive Power output within applicable Facility Ratings as directed by the Transmission Operator. In addition, WECC determined NAES's Transmission Operator did not exempt NAES from maintaining its generator voltage output as directed by the Transmission Operator.	VAR-002-1	R2	Medium	Severe	This violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) and posed a minimal risk to the BPS because NAES maintained stable output of the unit despite not having an Automatic Voltage Regulator (AVR) in service. In addition, the risk was further mitigated by the fact that this violation is applicable to a single 30 MW generation facility with limited to minimal capacity to boost system voltage during BPS disturbances. The generator involved in this violation represents a small fraction of the total generation available to the Transmission Operator. For this reason, WECC determined that any potential harm would also be minimal, assuming a complete failure did not happen concurrent with protection system (even an N-1) failure. Also, NAES operated in power factor mode in accordance with the generator's capability curve.	12/18/2008 (when the Transmission Operator originally distributed the voltage schedule)	1/4/2011	$3,500 (for WECC201002403 and WECC201002404)	Self-Report	On February 2, 2011, NAES submitted a Mitigation Plan. NAES contacted its Transmission Operator to ensure the voltage schedule on hand was the latest version. After review of the voltage schedule that was provided, NAES requested and was granted a modified (lower) voltage schedule due to equipment limitations. NAES also revised its plant procedures for operation in accordance to the voltage schedule and trained its personnel involved with the activity.	1/4/2011	4/5/2011	Agrees and Stipulates to the Facts in the Settlement Agreement.	Mitigating Factors: NAES's internal compliance program is well-documented and supported by corporate management, NAES has a budget for compliance activities, it empowers its employees to report noncompliance to management, and NAES may elect to take disciplinary actions against employees involved in violations of the Reliability Standards. WECC did not consider two prior violations of VAR-002-1 R1 by NAES's affiliates--NAES Corporation - Lincoln Generating Facility (NOC-476) and NAES Corporation - Covert (NOC-808)--to be aggravating factors in determining the penalty amount because there was not a commonality of compliance responsibility among the NAES affiliates.
Western Electricity Coordinating Council (WECC)	Pacific Gas and Electric Company (PGAE)	NCR05299	WECC201002530	Notice of Confirmed Violation	On October 27, 2010, while conducting an internal quality assurance review, PGAE discovered possible noncompliance with COM-002-2 after reviewing its system dispatcher voice logs. On October 27, 2010, PGAE submitted a Self-Report addressing its possible noncompliance. A WECC subject matter expert (SME) reviewed the Self-Report. During the SME's review, PGAE provided its Quality Assurance report (QA report) that prompted PGAE's Self-Report. PGAE stated on the QA report "fifty-one conversations" between September 1, 2009 and June 30, 2010 did not include three way communication in accordance with this Standard. In a telephone interview with PGAE staff, the SME determined many of the 51 conversations described in the QA report did not involve "directives" as considered by this Standard. Therefore, WECC submitted a data request to PGAE asking for additional information related to the conversations. WECC specifically requested that PGAE identify which of the conversations described included operational or reliability directives. PGAE and the SME identified four of the conversations as directives. The SME verified that the personnel on the recordings are NERC-certified operators. The SME reviewed voice recordings of the four conversations. The SME determined PGAE appropriately used three way communication in three of the voice recordings. While reviewing voice recording 60793700050736 (recorded October 23, 2009), the SME determined PGAE personnel did not ensure the recipient of a directive relating to the Martin-Millbrae #1 115 kV line repeated the directive information back correctly. Therefore, the SME determined PGAE, as a Transmission Operator (TOP), was in possible violation of COM-002-2 R2. The SME forwarded the Self-Report, data request information, and the SME's findings to the WECC Compliance Enforcement Department (Enforcement). Enforcement reviewed the Self-Report, data request information, and the SME's findings. Enforcement determined PGAE issued directives in a clear, concise and definitive manner but PGAE's failure to ensure the recipient of the directive repeated the information back correctly is a violation of COM-002-2 R2.	COM-002-2	R2	Medium	High	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the bulk power system (BPS). PGAE did not use three way communication when it provided an operational directive, however, in this case the directive related to a planned outage discussion between a transmission and distribution dispatcher. The specific communication related to de-energizing a 115 kV line to enable a maintenance crew to work on a circuit breaker. As described above, PGAE issued the directive in a clear and concise manner, however, PGAE did not ensure the recipient repeated the information contained in the directive back. WECC determined, based on the voice recordings and SME's investigation, that PGAE used three way communication when issuing reliability directives. WECC determined PGAE's QA report, despite identifying 51 conversations with possible non-compliance with the Standard, demonstrated PGAE's operators use three way communication to prevent errors during normal and emergency operations.	10/23/2009	10/23/2009	$20,300 (combined for WECC201002530, WECC201102527)	Self Report	PGAE submitted a Mitigation Plan on January 11, 2011. To mitigate this violation, PGAE planned to revise its dispatch procedures to better define the role of dispatchers and the use of three way communication, establish internal reviews to ensure PGAE's operators maintain appropriate, compliant communication, conduct weekly peer reviews, quarterly supervisor reviews, and quarterly PGAE training team reviews of voice recordings and Quality Assurance spot checks of voice recordings. PGAE further plans to implement a record archival and retrieval system associated with dispatcher communication. PGAE also plans to prevent human errors through extensive training, including NERC Continuing Education Training (human performance and communication modules). WECC reviewed the mitigation plan. WECC determined the timeframe for PGAE to complete operator training (milestone expected to be completed as of January 1, 2012), was not timely and contacted PGAE staff. PGAE's NERC Compliance Manager stated PGAE management is committing to completing the training earlier and that the reviews outlined previously provide PGAE adequate time to ensure PGAE's training is effective. PGAE's mitigation plan is comprehensive and PGAE's NERC Compliance Manager indicated PGAE is committed to continuous improvement in three way communication, however WECC determined the mitigation plan documentation does not appropriately prioritize dispatcher training. In conversations with PGAE's NERC Compliance Manager, Enforcement determined PGAE's internal deadlines for completing the training did not match the timelines proposed in PGAE's mitigation plan. Enforcement determined PGAE's internal timeframe, wherein PGAE proposes to train the majority of its personnel on three way Communication by October and November 2011, reduces the risk this violation poses to the BPS. However, PGAE's mitigation plan does not require PGAE to complete such training until January 2012 and does not reference PGAE's internal deadlines. Accordingly, WECC rejected the mitigation plan. On May 31, 2011, WECC sent PGAE a Notice of Mitigation Plan Rejection. On the Notice of Mitigation Plan Rejection WECC stated "while PGAE's proposed plan includes several satisfactory achievements, it does not appropriately prioritize PGAE's tasks. Specifically, three-way communication involves human actions and PGAE's deadline for training its operators on three-way communication is January 2012." PGAE promptly responded, also on May 31, 2011, stating PGAE would submit a revised mitigation plan. PGAE submitted its revised Mitigation Plan on June 14, 2011.	10/6/2011 (Approved Date)	TBD	Admits	PGAE had an internal compliance program (ICP) which was a mitigating factor. The ICP was documented; disseminated throughout PGAE's operations staff; had an oversight staff which was supervised at a high level in the organization and it has independent access to the CEO and/or board of directors; the ICP is operated such that it is independent of staff responsible for compliance of Standards; supported and participated by senior management; reviewed and modified regularly; includes formal, internal self-auditing of Standards on a periodic basis; and includes disciplinary action for employees involved in violations of the Standards.
Western Electricity Coordinating Council (WECC)	Pacific Gas and Electric Company (PGAE)	NCR05299	WECC201102527	Notice of Confirmed Violation	On March 7, 2011, in reviewing an internal monthly compliance report PGAE discovered that oil samples on Midway 500 kV shunt reactors were completed four days past the compliance due date. No incident or impact to the BPS occurred. These reactors are located on Path 15, South of Los Banos or Midway-Los Banos. The SME determined PGAE's Transmission Maintenance and Inspection Plan (TMIP) required PGAE to sample the line reactor oil to ensure the internal functions of the reactors operate properly. Such sampling is compared to previous (and future) samples to verify the units remain in operable condition. PGAE, as a Transmission Owner and TOP, failed to sample the oil within the intervals defined in its TMIP, which resulted in the violation. This shunt reactor maintenance is part PG&E substation maintenance program in support of WECC Regional Standard PRC-STD-005-1 Requirement WR1.	PRC-STD-005-1	WR1	N/A *(PRC-STD-005-1, WR1 is a WECC Regional Reliability Standard)*	N/A *(PRC-STD-005-1, WR1 is a WECC Regional Reliability Standard)*	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the BPS. Oil samples were taken four days beyond the required interval. There were no events or equipment reliability impacts as a result of the late completion of this maintenance task.	2/1/2011	2/4/2011	$20,300 (combined for WECC201002530, WECC201102527)	Self Report	On May 27, 2011, PGAE submitted its Mitigation Plan. PGAE will complete the following actions to mitigate this violation: (1) refine and implement the roles and responsibilities of an Asset Strategist in support of Substation Maintenance headquarters; (2) develop and implement a Compliance Monitoring System; (3) deliver short-term training regarding PFC Standards to Substation and Maintenance and Testing personnel; (5) determine the extent of the scope; (6) develop and implement a more formalized long-term training program regarding the substation maintenance program and NERC/WECC compliance requirements. PGAE will implement the following to prevent future risk to the BPS: (1) a Training and Monitoring System, by having consistent training of the modified reports and monitoring system it will ensure that required maintenance to the BPS will be performed per PGAE's documented maintenance cycles; and (2) Validation of SAP Work Management System, which will ensure that changes to headquarter or substation assignments reflect required maintenance work.	11/1/2011 (Approved Date)	TBD	Admits	PGAE had an ICP which was a mitigating factor. The ICP was documented; disseminated throughout PGAE's operations staff; had an oversight staff which was supervised at a high level in the organization and it has independent access to the CEO and/or board of directors; the ICP is operated such that it is independent of staff responsible for compliance of Standards; supported and participated by senior management; reviewed and modified regularly; includes formal, internal self-auditing of Standards on a periodic basis; and includes disciplinary action for employees involved in violations of the Standards.
Western Electricity Coordinating Council (WECC)	Thermo Power and Electric LLC (THPE)	NCR05425	WECC200901621	Settlement Agreement	On August 4, 2009, THPE submitted a Self-Certification reporting it was in violation of CIP-001-1 R1. The noncompliance was discovered as a result of a third-party gap analysis performed for THPE to determine its overall NERC compliance status. WECC determined that THPE, as a Generator Operator, failed to ensure that current THPE sabotage reporting documentation contained procedures for the recognition of sabotage procedures, for the communication of information concerning sabotage to the appropriate parties within the interconnection, or sabotage response guidelines, as required by the Standard.	CIP-001-1	R1	Medium	Severe	THPE instructed facility personnel to remain vigilant and report any suspicious activity while THPE develops and implements updated sabotage procedures. Furthermore, THPE operates a single generating facility with three small generators that combine for approximately 80 MWs of generating capacity. In addition, THPE does not operate the generators at full capacity, but rather operates in limited circumstances pursuant to its power purchase contracts. THPE's generation is fraction of the generation available to the transmission operation and an even smaller fraction of the generation available to the Balancing Authority. For these reasons, WECC believes this violation poses a minimal risk to the reliability of the bulk power system (BPS).	6/18/2007 (date Standard was enforceable)	9/8/2009 (date THPE completed Mitigation Plan)	$10,000 (for WECC200901621, WECC200901622, WECC200901623, WECC200901637, and WECC200901553)	Self-Certification	THPE stated in its mitigation plan that it would work with a third party vendor to develop robust sabotage reporting procedures that would address the requirements of CIP-001-1 R1, R2 and R3. THPE submitted its *Sabotage Reporting Procedures* and a personnel training log detailing the procedures required by CIP-001-1 R1, R2 and R3. WECC determined THPE developed procedures for the recognition and for making of its personnel aware of sabotage events on THPE facilities and multi-site sabotage affecting larger portions of the Interconnection, including procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. WECC determined the personnel training log demonstrated THPE provided its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	9/8/2009	12/31/2009	Agree and Stipulates to the Facts in the Settlement Agreement	WECC considered THPE's internal compliance program (ICP) as a mitigating factor in assessing the penalty. WECC found that THPE's ICP is documented; THPE has ICP oversight staff; ICP oversight staff is supervised at a high level in the organization; THPE has allocated resources to Its ICP; the ICP has the support and participation of senior management; THPE reviews its ICP on an annual basis; THPE's ICP Includes formal, Internal self-auditing for compliance with all Reliability Standards on a periodic basis; and THPE's Compliance Department includes active engagement, and coordinated recurring meetings with, THPE senior management.

Attachment A-1
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Western Electricity Coordinating Council (WECC)	Thermo Power and Electric LLC (THPE)	NCR05425	WECC200901622	Settlement Agreement	On August 4, 2009, THPE submitted a Self-Certification reporting it was in violation of CIP-001-1 R2. The noncompliance was discovered as a result of a third-party gap analysis performed for THPE to determine its overall NERC compliance status. WECC determined that THPE, as a Generator Operator, failed to ensure that current THPE sabotage reporting documentation contained procedures for the recognition of sabotage procedures, for the communication of information concerning sabotage to the appropriate parties within the interconnection, or sabotage response guidelines, as required by the Standard.	CIP-001-1	R2	Medium	Severe	THPE instructed facility personnel to remain vigilant and report any suspicious activity while THPE develops and implements updated sabotage procedures. Furthermore, THPE operates a single generating facility with three small generators that combine for approximately 80 MWs of generating capacity. In addition, THPE does not operate the generators at full capacity, but rather operates in limited circumstances pursuant to its power purchase contracts. THPE's generation is fraction of the generation available to the transmission operation and an even smaller fraction of the generation available to the Balancing Authority. For these reasons, WECC believes this violation poses a minimal risk to the reliability of the BPS.	6/18/2007 (date Standard was enforceable)	9/8/2009 (date THPE completed Mitigation Plan)	$10,000 (for WECC200901621, WECC200901622, WECC200901623, WECC200901637, and WECC200901553)	Self-Certification	THPE stated in its mitigation plan that it would work with a third party vendor to develop robust sabotage reporting procedures that would address the requirements of CIP-001-1 R1, R2 and R3. THPE submitted its *Sabotage Reporting Procedures* and a personnel training log detailing the procedures required by CIP-001-1 R1, R2 and R3. WECC determined THPE developed procedures for the recognition and for making of its personnel aware of sabotage events on THPE facilities and multi-site sabotage affecting larger portions of the Interconnection, including procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. WECC determined the personnel training log demonstrated THPE provided its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	9/8/2009	12/31/2009	Agree and Stipulates to the Facts in the Settlement Agreement	WECC considered THPE's ICP as a mitigating factor in assessing the penalty. WECC found that THPE's ICP is documented; THPE has ICP oversight staff; ICP oversight staff is supervised at a high level in the organization; THPE has allocated resources to Its ICP; the ICP has the support and participation of senior management; THPE reviews its ICP on an annual basis; THPE's ICP Includes formal, Internal self-auditing for compliance with all Reliability Standards on a periodic basis; and THPE's Compliance Department includes active engagement, and coordinated recurring meetings with, THPE senior management.
Western Electricity Coordinating Council (WECC)	Thermo Power and Electric LLC (THPE)	NCR05425	WECC200901623	Settlement Agreement	On August 4, 2009, THPE submitted a Self-Certification reporting it was in violation of CIP-001-1 R3. The noncompliance was discovered as a result of a third-party gap analysis performed for THPE to determine its overall NERC compliance status. WECC determined that THPE, as a Generator Operator, failed to ensure that current THPE sabotage reporting documentation contained procedures for the recognition of sabotage procedures, for the communication of information concerning sabotage to the appropriate parties within the interconnection, or sabotage response guidelines, as required by the Standard.	CIP-001-1	R3	Medium	Severe	THPE instructed facility personnel to remain vigilant and report any suspicious activity while THPE develops and implements updated sabotage procedures. Furthermore, there have been no incidents of sabotage at THPE's facilities, and thus no actual impact to the BPS. For these reasons, WECC believes this violation poses a minimal risk to the reliability of the BPS.	6/18/2007 (date Standard was enforceable)	9/8/2009 (date THPE completed Mitigation Plan)	$10,000 (for WECC200901621, WECC200901622, WECC200901623, WECC200901637, and WECC200901553)	Self-Certification	THPE stated in its mitigation plan that it would work with a third party vendor to develop robust sabotage reporting procedures that would address the requirements of CIP-001-1 R1, R2 and R3. THPE submitted its *Sabotage Reporting Procedures* and a personnel training log detailing the procedures required by CIP-001-1 R1, R2 and R3. WECC determined THPE developed procedures for the recognition and for making of its personnel aware of sabotage events on THPE facilities and multi-site sabotage affecting larger portions of the Interconnection, including procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection. WECC determined the personnel training log demonstrated THPE provided its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	9/8/2009	12/31/2009	Agree and Stipulates to the Facts in the Settlement Agreement	WECC considered THPE's ICP as a mitigating factor in assessing the penalty. WECC found that THPE's ICP is documented; THPE has ICP oversight staff; ICP oversight staff is supervised at a high level in the organization; THPE has allocated resources to Its ICP; the ICP has the support and participation of senior management; THPE reviews its ICP on an annual basis; THPE's ICP Includes formal, Internal self-auditing for compliance with all Reliability Standards on a periodic basis; and THPE's Compliance Department includes active engagement, and coordinated recurring meetings with, THPE senior management.
Western Electricity Coordinating Council (WECC)	Thermo Power and Electric LLC (THPE)	NCR05425	WECC200901637	Settlement Agreement	On August 4, 2009, THPE submitted a Self-Certification reporting it was in violation of FAC-008-1 R1. WECC determined that THPE, as a Generator Owner, failed to have a process for documenting its Facility Rating Methodology, as required by the Standard. In addition, WECC found that THPE did not have the Facility Rating statement, as required by R1.1. WECC also determined that THPE did not have a method for the determination of a Facility Rating and the scope of equipment covered by those Ratings, for its solely and jointly owned Facilities, as required by R1.2 of the Standard. WECC also determined that THPE did not have Facility Ratings that considered the Ratings provided by manufacturers, design criteria, ambient conditions and operating limitations, as required by R1.3 of the Standard.	FAC-008-1	R1	Medium	Severe	THPE reported that it did not have a Facility Ratings Methodology for its solely and jointly owned Facilities; however, THPE operates a single generating facility with three small generators that combine for approximately 80 MW of generating capacity. In addition, THPE does not operate the generators at full capacity, but rather operates in limited circumstances pursuant to its power purchase contracts. THPE's generation is fraction of the generation available to the transmission operator and an even smaller fraction of the generation available to the Balancing Authority. For these reasons, WECC believes this violation poses a minimal risk to the reliability of the BPS.	6/18/2007 (date Standard was enforceable)	9/11/2009 (date THPE completed Mitigation Plan)	$10,000 (for WECC200901621, WECC200901622, WECC200901623, WECC200901637, and WECC200901553)	Self-Certification	THPE stated in its mitigation plan that it hired a third-party consultant to assist in the development of a Facility Rating Methodology. THPE submitted a mitigation plan completion form and it's *Facility Ratings Methodology Via Electrical Component Analysis* to WECC as evidence of compliance. THPE WECC determined THPE documented its current methodology used for developing Facility Ratings of its solely and jointly owned facilities. WECC further determined such methodology Included each of the subcomponents of FAC-008-1 R1.	9/11/2009	11/4/2009	Agree and Stipulates to the Facts in the Settlement Agreement	WECC considered THPE's ICP as a mitigating factor in assessing the penalty. WECC found that THPE's ICP is documented; THPE has ICP oversight staff; ICP oversight staff is supervised at a high level in the organization; THPE has allocated resources to Its ICP; the ICP has the support and participation of senior management; THPE reviews its ICP on an annual basis; THPE's ICP Includes formal, Internal self-auditing for compliance with all Reliability Standards on a periodic basis; and THPE's Compliance Department includes active engagement, and coordinated recurring meetings with, THPE senior management.
Western Electricity Coordinating Council (WECC)	Thermo Power and Electric LLC (THPE)	NCR05425	WECC200901553	Settlement Agreement	On August 4, 2009, THPE submitted a Self-Certification reporting it was in violation of FAC-009-1 R1. WECC determined that THPE, as a Generator Owner, failed to develop Facility Ratings for its solely and jointly owned Facilities that were consistent with the associated Facility Ratings Methodology, as required by R1 of the Standard.	FAC-009-1	R1	Medium	Severe	THPE reported that it did not have a Facility Ratings Methodology for its solely and jointly owned Facilities; however, THPE operates a single generating facility with three small generators that combine for approximately 80 MW of generating capacity. In addition, THPE does not operate the generators at full capacity, but rather operates in limited circumstances pursuant to its power purchase contracts. THPE's generation is fraction of the generation available to the transmission operator and an even smaller fraction of the generation available to the Balancing Authority. For these reasons, WECC believes this violation poses a minimal risk to the reliability of the bulk power system (BPS).	6/18/2007 (date Standard was enforceable)	10/1/2009 (date THPE completed Mitigation Plan)	$10,000 (for WECC200901621, WECC200901622, WECC200901623, WECC200901637, and WECC200901553)	Self-Certification	THPE stated in its mitigation plan that it had hired a third-party consultant to assist in the development of Facility Ratings once a Facility Rating Methodology had been developed. WECC determined THPE established Facility Ratings for its solely and jointly owned Facilities that are consistent with the associated Facility Ratings Methodology.	10/1/2009	12/31/2009	Agree and Stipulates to the Facts in the Settlement Agreement	WECC considered THPE's ICP as a mitigating factor in assessing the penalty. WECC found that THPE's ICP is documented; THPE has ICP oversight staff; ICP oversight staff is supervised at a high level in the organization; THPE has allocated resources to Its ICP; the ICP has the support and participation of senior management; THPE reviews its ICP on an annual basis; THPE's ICP Includes formal, Internal self-auditing for compliance with all Reliability Standards on a periodic basis; and THPE's Compliance Department includes active engagement, and coordinated recurring meetings with, THPE senior management.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000692	Settlement Agreement	RFC_URE1 submitted a Self-Report to ReliabilityFirst stating that its security monitoring process failed to detect and alert for unauthorized access attempts for two firewalls located on an electronic security perimeter (ESP). Specifically, RFC_URE1's security management software tool was configured to alert RFC_URE1 to unauthorized access attempts based upon a threshold frequency of access denials from a specific IP address. RFC_URE1 did not configure two firewalls to report access denial events to the security management software tool. As a result, RFC_URE1's security logging and alerts would not have functioned correctly if there had been unauthorized access attempts to the firewalls.	CIP-005-1	R3/ R3.2	Medium	Severe	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because RFC_URE1 configured the firewalls on the ESP to deny access by default, and therefore the Critical Cyber Assets (CCAs) within the ESP remained protected from unauthorized access attempts throughout the duration of the violation. Additionally, the security management software tool did log all permitted access attempts and firewall configuration changes.	The date on which RFC_URE1 was subject to compliance with CIP-005-1.	The date on which RFC_URE1 corrected the configuration of the firewalls to log and report access denial events to the security management tool.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Self-Report	RFC_URE1 corrected the configuration of its firewalls to log and alert RFC_URE1 to all denied unauthorized access attempts.	10/12/2010	8/17/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000693	Settlement Agreement	RFC_URE1 submitted a Self-Report to ReliabilityFirst stating that it discovered a network switch that had ports and services that were not required for normal or emergency operations but that were still enabled, in violation of CIP-007-1 R2. While performing an annual vulnerability assessment, RFC_URE1 discovered that the network switch, which is located inside the electronic security perimeter (ESP), had ports and services that were not required for normal and emergency operations, but that were still enabled	CIP-007-1	R2/ R2.1, R2.2	Medium	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the network switch is located behind the ESP firewall and is therefore not accessible from outside the ESP.	The date on which RFC_URE1 was subject to compliance with CIP-007-1.	The date on which RFC_URE1 disabled the ports and services that were enabled on the network switch.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Self-Report	RFC_URE1 disabled the ports and services that were enabled on the network switch.	11/19/2010	8/16/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000694	Settlement Agreement	RFC_URE1 submitted a Self-Report to ReliabilityFirst stating that it failed to remove or disable factory default accounts on a network switch (the same network switch as RFC201000693), and failed to meet password requirements as required by CIP-007-1 R5. Specifically, RFC_URE1 discovered a network switch within the electronic security perimeter (ESP) had two factory default accounts that RFC_URE1 had not removed, disabled, or renamed. Additionally, RFC_URE1 failed to create passwords for the two factory default accounts that conform with the requirements of CIP-007-1 R5.3, prior to placing them into service. RFC_URE1 discovered this oversight during its annual vulnerability assessment.	CIP-007-1	R5	Lower	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the network switch containing the two factory default accounts is located behind the ESP firewall and is therefore not accessible from outside the ESP.	The date on which RFC_URE1 was subject to compliance with CIP-007-1.	The date on which RFC_URE1 set complex passwords for the two factory default accounts on the network switch.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Self-Report	RFC_URE1 set complex passwords for the two factory default accounts on the network switch that conform to CIP-007-1 R5.3.	11/19/2010	8/16/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100752	Settlement Agreement	ReliabilityFirst conducted a compliance audit of RFC_URE1 (the Compliance Audit). During the Compliance Audit, ReliabilityFirst discovered that RFC_URE1's physical security plan failed to satisfy two requirements of CIP-006-1. First, RFC_URE1's physical security plan failed to address response to loss and prohibition of inappropriate use of physical access controls, as required by CIP-006-1 R1.4. Second, RFC_URE1's physical security plan stated that it would be updated within 90 calendar days of a physical security system design or configuration change. Although Version 1 of CIP-006, R1.7 allowed for a 90-day period to update a physical security plan, on April 1, 2010 Version 2 of CIP-006 took effect, which requires a narrower, 30-day update period. Therefore, from the effective date of CIP-006-2, RFC_URE1 failed to include a requirement in its physical security plan to update the physical security plan within 30 days of a physical security system design or configuration change.	CIP-006-1	R1/ R1.4, R1.7	Medium	Severe	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because although RFC_URE1's physical security plan did not include information about responding to loss or a prohibition of inappropriate use of physical access controls, RFC_URE1 addressed these topics in another RFC_URE1 document, and trained its employees on these topics. Additionally, although RFC_URE1's physical security plan stated that RFC_URE1 must update the physical security plan within 90 days of any changes rather than within 30 days, RFC_URE1 made no changes to its physical security plan during the duration of this violation, and did not need to make any updates.	The date on which RFC_URE1 was required to be compliant with CIP-006-1.	The date on which RFC_URE1 revised its physical security plan to comply with CIP-006-1 R1.4 and R1.7.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Compliance Audit	RFC_URE1 revised its physical security plan to address response to loss and prohibition of inappropriate use of physical access controls, and to include a requirement to update the physical security plan within 30 days of a physical security system design or configuration change.	1/27/2011	8/19/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100753	Settlement Agreement	ReliabilityFirst conducted a compliance audit of RFC_URE1 (the Compliance Audit). During the Compliance Audit, ReliabilityFirst discovered that RFC_URE1's Cyber Security incident response plan failed to include a process for updating the Cyber Security incident response plan within 30 calendar days of any changes. Instead, RFC_URE1's Cyber Security incident response plan included a process for updating the Cyber Security incident response plan within 90 calendar days of any changes. Although Version 1 of CIP-008 allowed for a 90-day period to update the Cyber Security incident response plan, on April 1, 2010 Version 2 of CIP-008 took effect, which requires a narrower, 30-day period. Therefore, from the effective date of CIP-008-2, RFC_URE1 failed to comply with CIP-008-2 R1.4.	CIP-008-2	R1	Lower	High	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because although RFC_URE1's Cyber Security incident response plan stated that RFC_URE1 must update the Cyber Security incident response plan within 90 days of any changes rather than within 30 days, RFC_URE1 made no changes to the Cyber Security incident response plan during the time period of this violation, and therefore, did not need to make any updates.	The date on which RFC_URE1's Cyber Security incident response plan was not compliant with the updated Version 2 of CIP-008.	The date on which RFC_URE1 revised its Cyber Security incident response plan to include a process for updating the Cyber Security incident response plan within 30 calendar days of changes.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Compliance Audit	RFC_URE1 revised its Cyber Security incident response plan to include a process for updating the Cyber Security incident response plan within 30 calendar days of any changes.	1/27/2011	8/12/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100754	Settlement Agreement	ReliabilityFirst conducted a compliance audit of RFC_URE1 (the Compliance Audit). During the Compliance Audit, ReliabilityFirst discovered that RFC_URE1's recovery plan failed to satisfy both sub-requirements of CIP-009-1 R1. First, RFC_URE1's recovery plan failed to specify events or conditions of varying duration and severity that would activate the recovery plan, as required by R1.1. Second, RFC_URE1's recovery plan failed to define the roles and responsibilities of responders, as required by R1.2. In addition, RFC_URE1 failed to address all of its Critical Cyber Assets (CCAs) in its recovery plan. The plan addressed only six of RFC_URE1's 13 total CCAs.	CIP-009-1	R1	Medium	Severe	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because although RFC_URE1 did not specify events or conditions of varying duration and severity that would activate the recovery plan, it did address responding to events of varying duration and severity in its CIP-008 Cyber Security Incident response plan. Similarly, although RFC_URE1 did not define the roles and responsibilities of responders in its recovery plan, it did address those roles and responsibilities in its CIP-003 cyber security policy. RFC_URE1 represents that the information that it failed to specifically state within its recovery plan would have been readily available to authorized RFC_URE1 personnel responding to an event requiring the recovery of CCAs.	The date on which RFC_URE1 was required to be compliant with CIP-009-1.	The date on which RFC_URE1 revised its recovery plan to comply with CIP-009-1 R1.	$30,000 (for RFC201000692, RFC201000693, RFC201000694, RFC201100752, RFC201100753, and RFC201100754)	Compliance Audit	RFC_URE1 revised its recovery plan to specify events or conditions of varying duration and severity that would activate the recovery plan, define the roles and responsibilities of responders, and address all of RFC_URE1's CCAs.	1/27/2011	8/16/2011	Neither Admits nor Denies	RFC_URE1 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor.
Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201000689	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-004-2 R4.1, due to RFC_URE2's failure to update the list of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets within seven days of a change of personnel with such access to Critical Cyber Assets. Specifically, RFC_URE2 terminated an employee for cause but did not update the list of personnel with access to Critical Cyber Assets within seven days of the change in access rights. Nevertheless, RFC_URE2 did revoke the terminated employee's access within 24 hours, as required by CIP-004-2 R4.2. RFC_URE2 violated CIP-004-2 R4.1 by failing to update the list of personnel who have access to Critical Cyber Assets within seven days of any change of personnel with such access to Critical Cyber Assets.	CIP-004-2	R4 (R4.1)	Lower	High	ReliabilityFirst determined the violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because RFC_URE2 revoked access control cards, passwords, and appropriate accounts from the terminated employee within twenty-four hours of the employee's termination. In addition, while the terminated employee was on the list of personnel who have access to Critical Cyber Assets because of his access to electronic confidential records, the employee did not have electronic access or control privileges to the Supervisory Control and Data Acquisition (SCADA) system or any other Critical Cyber Assets.	The date by which RFC_URE2 was required to update its Critical Cyber Assets access list.	The date on which RFC_URE2 updated its list of personnel with access to Critical Cyber Assets to remove the terminated individual.	$1,000 (Settlement for RFC201000689)	Self-Report	RFC_URE2 updated its list of personnel with access to Critical Cyber Assets to reflect the updated accesses to Critical Cyber Assets. In addition, RFC_URE2 informed all managers of the need to report the change in status of any employee on the CIP confidential list.	1/4/2011	5/24/2011	Agrees and Stipulates to the Facts	Reliability*First* determined that there was nothing in the record to suggest that broader corporate issues were implicated.
Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201000457	Settlement Agreement	RFC_URE3 submitted a Self-Report to ReliabilityFirst concerning a violation of CIP-005-1 R3.2. RFC_URE3's internal computer network supports RFC_URE3's Energy Management Systems (EMS). RFC_URE3's interior firewalls separate the internal computer network from its general business network. The interior firewalls serve as the Electronic Security Perimeter (ESP) for RFC_URE3's internal computer network, as well as the access points to the ESP. While conducting an internal review , RFC_URE3 discovered that it had not fully enabled its logging and alerting system to alert for unauthorized access attempts to the ESP, as required by CIP-005-1 R3.2. ReliabilityFirst determined RFC_URE3 failed to implement its processes for monitoring and logging access at access points to the ESP. Specifically, RFC_URE3 failed to enable its logging and alert system for attempts at or actual unauthorized access to RFC_URE3's ESP, as required by CIP-005-1 R3.2.	CIP-005-1	R3 (R3.2)	Medium	Severe	ReliabilityFirst determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because, for the duration of the violation, RFC_URE3's internal computer network was monitored by two intrusion detection software products. Although RFC_URE3's intrusion detection software did not monitor ESP access points, in the event of actual unauthorized access to or suspicious behavior on RFC_URE3's ESP, the intrusion detection software would detect the intrusion or suspicious behavior and notify RFC_URE3. In addition, RFC_URE3 reviewed logs from January 1, 2010, through August 12, 2010, the date RFC_URE3 reconfigured its ESP settings to comply with CIP-005-1, R3.2, and found that there were no attempts to access the ESP from any unauthorized IP addresses.	The date RFC_URE3 failed to implement its processes for monitoring and logging access points to the ESP.	The date RFC_URE3 fully enabled detection and alerting for unauthorized access attempts on its ESP.	$6,000 (Settlement of RFC201000457)	Self-Report	RFC_URE3 reconfigured its ESP to send system logging alerts to the administrator and supervisor of the EMS . In addition, RFC_URE3 conducted a test to ensure all configured controls were working as required, which was successful. Finally, RFC_URE3 now retains all logs for a rolling 365-day cycle and all alerts for a minimum of 90 days.	8/12/2010	5/13/2011	Neither Admits nor Denies	ReliabilityFirst considered certain aspects of RFC_URE3's compliance program as mitigating factors.
Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201000395	Settlement Agreement	During a Spot Check of RFC_URE4, Reliability*First* determined that RFC_URE4 failed to identify six of its Cyber Assets that either use a routable protocol to communicate outside the Electronic Security Perimeter or use a routable protocol within a control center as Critical Cyber Assets. First, RFC_URE4 failed to identify four remote workstations that communicate outside the Electronic Security Perimeter using a routable protocol as Critical Cyber Assets, in violation of CIP-002-1 R3.1. These four remote workstations are enabled to monitor and control the bulk power system (BPS). Second, RFC_URE4 also failed to identify two of its workstations, which use a routable protocol within a control center as Critical Cyber Assets, in violation of CIP-002-1 R3.2. (RFC_URE4 did, however, list the two workstations as Cyber Assets.)	CIP-002-1	R3	High	Severe	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. All users of the six workstations at issue had completed personnel risk assessments and had authorized access to Critical Cyber Assets. The four workstations that used a routable protocol to communicate outside the Electronic Security Perimeter utilized three levels of password protection, which provided protection against unauthorized users from utilizing the workstations to control any BPS assets. The two workstations that used a routable protocol within a control center remained within the Physical Security Perimeter and the Electronic Security Perimeter, and therefore received all the same protections as Critical Cyber Assets.	The date on which RFC_URE4 was subject to compliance with CIP-002-1 R3.	The date on which RFC_URE4 reconfigured its workstations.	$16,500 (for RFC201000395, RFC201000398, and RFC201000399)	Spot Check	On August 31, 2010, RFC_URE4 submitted to Reliability*First* its mitigation plan to address the violation of CIP-002-1 R3. In this mitigation plan, RFC_URE4 memorialized the actions it took to address the violation of CIP-002-1 R3. RFC_URE4 reconfigured the four workstations that communicated outside the Electronic Security Perimeter, and removed their control functionality. These four workstations are currently not classified as Critical Cyber Assets, since they are now limited to monitoring functions and are therefore not "essential to the operation of the Critical Asset." RFC_URE4 also added the two workstations that use a routable protocol within the control center to the RFC_URE4 Critical Cyber Asset list.	6/23/2010	10/22/2010	Admits	Reliability*First* considered RFC_URE4's internal compliance program (ICP) as a mitigating factor in assessing the penalty.

City of Vineland New Jersey

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201000398	Settlement Agreement	During a Spot Check, Reliability*First* determined that RFC_URE4 failed to ensure that a significant change to existing Cyber Assets within the Electronic Security Perimeter did not adversely affect existing security controls. Specifically, Reliability*First* examined evidence of a software upgrade, including RFC_URE4's testing of the software upgrade, but the evidence of testing did not provide sufficient information to establish that the software upgrade did not adversely affect RFC_URE4's cyber security controls. RFC_URE4 provided evidence of later testing of the software upgrade, which showed significant discrepancies from the evidence of the original testing.	CIP-007-1	R1	Medium	High	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). RFC_URE4 utilizes two fully redundant systems at its primary location and two fully redundant systems at its backup location. These systems are upgraded at different times, thereby providing protection in the event of adverse effects from the software upgrade.	The date on which RFC_URE4 implemented a change to existing Cyber Assets within the ESP without ensuring that the change did not adversely affect existing security controls.	The date on which RFC_URE4 documented testing of cyber security controls.	$16,500 (for RFC201000395, RFC201000398, and RFC201000399)	Spot Check	On August 31, 2010, RFC_URE4 submitted to Reliability*First* its mitigation plan to address the violation of CIP-007-1 R1. In this mitigation plan, RFC_URE4 memorialized the actions it took to address the violation of CIP-007-1 R1. RFC_URE4 created a check list for documenting all future testing of changes to Cyber Assets to ensure that it properly tests security controls both before and after the changes to Cyber Asset are made.	6/22/2010	10/22/2010	Admits	Reliability*First* considered RFC_URE4's internal compliance program (ICP) as a mitigating factor in assessing the penalty.
Unidentified Registered Entity 4 (RFC_URE4)	NCRXXXXX	RFC201000399	Settlement Agreement	During a Spot Check, Reliability*First* determined that RFC_URE4 failed to demonstrate that it annually tested its Cyber Security Incident response plan. Therefore, RFC_URE4 failed to ensure that its Cyber Security Incident response plan is tested at least annually. Reliability*First* found that RFC_URE4 violated CIP-008-1 R1.6 by failing to ensure that its Cyber Security Incident response plan is tested at least annually.	CIP-008-1	R1.6	Lower	High	Reliability*First* determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although, RFC_URE4 did not produce sufficient documentation at the Spot Check to establish compliance with CIP-008-1 R1, RFC_URE4 represents that it tested the Cyber Security Incident response plan. Furthermore, RFC_URE4 has conducted a recent test of the Cyber Security Incident response plan, which demonstrates the efficacy of the Cyber Security Incident response plan in responding to incidents.	The date on which RFC_URE4 was subject to compliance with CIP-008-1 R1.	The date on which RFC_URE4 developed a test report form for its Cyber Security Incident response plan.	$16,500 (for RFC201000395, RFC201000398, and RFC201000399)	Spot Check	On August 31, 2010, RFC_URE4 submitted to Reliability*First* its mitigation plan to address the violation of CIP-008-1 R1.6. RFC_URE4 memorialized the actions it took to address the violation of CIP-008-1 R1.6. RFC_URE4 developed a test report form to cover all steps required in RFC_URE4's Cyber Security Incident response plan.	6/21/2010	10/22/2010	Admits	Reliability*First* considered RFC_URE4's internal compliance program (ICP) as a mitigating factor in assessing the penalty.
Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000393	Settlement Agreement	RFC_URE5 submitted a Self-Report indicating a violation of CIP-004-1 R4.2, to ReliabilityFirst. RFC_URE5 failed to remove one employee (Employee A) which no longer required access to CCAs from their Critical Cyber Asset (CCA) Electronic Access List within seven days. On March 22, 2010, RFC_URE5 designated Employee A as inactive but did not remove CCA electronic access or update the CCA Electronic Access List until May 11, 2010. RFC_URE5 submitted a Self-Report update indicating that the violation of CIP-004-1 R4.2 expanded in scope. RFC_URE5 did not remove an additional employee (Employee B) from its CCA Physical Access list within seven days of Employee B no longer requiring access. Specifically, Employee B resigned from the company effective August 7, 2010, but was not removed from the Physical Access List until August 18, 2010. RFC_URE5 did revoke all access rights for Employee B on August 7, 2010. RFC_URE5 submitted a second update to the Self-Report. RFC_URE5 granted an employee (Employee C) temporary access to a Physical Security Perimeter (PSP) from June 2, 2010 to June 4, 2010, but failed to remove Employee C from the CCA Physical Access List within seven calendar days of revoking Employee C's access on June 4, 2010. RFC_URE5 did not remove Employee C from the CCA Physical Access List until September 21, 2010. RFC_URE5 violated CIP-004-1 R4 on three separate occasions when it failed to remove Employees A, B and C from its CCA Access Lists within seven days of those employees no longer requiring access to CCAs.	CIP-004-1	R4/ R4.2	Medium	Moderate	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Employee A did not have physical access to the PSP in which the CCAs reside during the time period of the violation. Moreover the CCAs could not be electronically accessed by Employee A from anywhere outside the PSP. Employee B did not have physical access to the PSP during the time period of the violation. RFC_URE5 collected all access devices that would allow Employee B to physically enter the PSP on the same day as Employee B resigned. As a result, it was impossible for Employee B to physically access the PSP after August 7, 2010. Employee B also had completed CIP training and had a clear personnel risk assessment (PRA) in place at the time of the violation. Although Employee C did have key card access to the PSP, Employee C did not have key access to the perimeter gate surrounding the PSP, and did not have a non-forcible means of access to the perimeter gate surrounding the PSP. Additionally, Employee C had completed CIP training and had a clear PRA in place at the time of the violation.	The date by which RFC_URE5 should have removed Employee A from the CCA Electronic Access List.	The date RFC_URE5 removed Employee C from the CCA Physical Access List.	$30,000 (for RFC201000393, RFC201000394, and RFC201000773)	Self-Report	RFC_URE5 updated the CCA Access Lists to reflect the personnel status changes for Employees A, B, and C. RFC_URE5 also removed Employee C's key access to the PSP. RFC_URE5 reviewed the incidents of non-compliance and the procedures that were not followed, and then revised those procedures. Senior management from the Human Resources and Legal departments reinforced the importance of adhering to the CIP procedures to the entire company. RFC_URE5 developed a process to compare its Human Resources personnel database with the database used to identify roles in the CIP Compliance program. RFC_URE5 now generates a daily report to identify any changes in the status of an employee with physical or electronic access to the PSP.	2/22/2011	6/7/2011	Neither Admits nor Denies	The parent company of RFC_URE5 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor. RFC_URE5 does not have any prior violations of the CIP Reliability Standards. ReliabilityFirst did consider the repetitive nature of the violations addressed within this Settlement Agreement as an aggravating factor in the penalty determination. In considering the instant violations, ReliabilityFirst did not observe any evidence of involvement of the entire holding company system or other affiliates.
Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000394	Settlement Agreement	RFC_URE5 submitted a Self-Report indicating a violation of CIP-006-1 R2 to ReliabilityFirst. On March 31, 2010, a RFC_URE5 employee with authorized unescorted physical access to a Physical Security Perimeter (PSP) (Authorized Employee) failed to manage a PSP access point on three occasions, for a combined duration of approximately 15 minutes. Individuals without authorized access were performing maintenance on the floor below the PSP access point, and as a result of the maintenance, RFC_URE5 left the door that is used to secure the PSP ajar. During the time period that the door to the PSP was ajar, the Authorized Employee left the area on three occasions and failed to monitor this PSP access point. RFC_URE5 violated CIP-006-1 R2 by failing to implement its physical security plan and manage physical access to all access points to the PSP.	CIP-006-1	R2	Medium	High	ReliabilityFirst determined this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system to the reliability of the bulk power system because RFC_URE5 had a documented Physical Security Plan in place that addressed the requirement to control access points to the PSP, and trained the Authorized Employee on this requirement. The PSP access point is located within an access-controlled facility and also within a further restricted, access-controlled, corporate data center. Therefore, the PSP access point has multiple layers of protection. The PSP is also under video surveillance, which allowed RFC_URE5 to monitor any attempts by an unauthorized individual to enter through this PSP access point. No such attempts were made during the alleged violation. Finally, the violation was short in duration, lasting approximately 15 minutes.	The time period which RFC_URE5 failed to manage physical access to a PSP for 15 minutes.	When RFC_URE5 returned to monitoring physical access to the PSP.	$30,000 (for RFC201000393, RFC201000394, and RFC201000773)	Self-Report	RFC_URE5 enhanced its Physical Security Plan, and developed a targeted CIP training session specifically for business services employees who may be involved in maintenance activities at PSP access points. The CIP training session reinforced the companies' visitor escort policy and clarified the requirements for monitoring PSP access points. RFC_URE5 conducted additional CIP training sessions for RFC_URE5 employees and contractors. RFC_URE5 also posted signs at PSP access points and distributed laminated cards to remind employees and contractors that access is restricted to authorized individuals, and detail requirements for access control, visitor escorting, and entry logging.	8/30/2010	4/13/2011	Neither Admits nor Denies	The parent company of RFC_URE5 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor. RFC_URE5 does not have any prior violations of the CIP Reliability Standards. ReliabilityFirst did consider the repetitive nature of the violations addressed within this Settlement Agreement as an aggravating factor in the penalty determination. In considering the instant violations, ReliabilityFirst did not observe any evidence of involvement of the entire holding company system or other affiliates.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 5 (RFC_URE5)	NCRXXXXX	RFC201000773	Settlement Agreement	RFC_URE5 submitted a Self-Report indicating a violation of CIP-004-1 R3 to ReliabilityFirst. On October 1, 2010, RFC_URE5 discovered that it provided an employee (Employee 1) with authorized unescorted physical access to a Physical Security Perimeter (PSP) on January 1, 2010, who did not have a personnel risk assessment (PRA) within 30 days of access. On October 1, 2010, RFC_URE5 also discovered that it provided a second employee (Employee 2) with authorized unescorted physical access to a PSP on April 15, 2010, who did not have a PRA within 30 days of access. Finally, on October 14, 2010, RFC_URE5 discovered that it provided a third employee (Employee 3) with authorized unescorted physical access to a PSP on October 13, 2010, who did not have a PRA within 30 days of access. RFC_URE5 violated CIP-004-1 R3 by failing to conduct PRAs for three employees within 30 days of providing those employees with authorized access to a PSP.	CIP-004-1	R3	Medium	High	ReliabilityFirst determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system because Employee 1 and Employee 2 did not enter the PSP during the time period of the violation. Additionally, RFC_URE5 later conducted PRAs for Employee 1,2, and 3, which identified no issues. Employee 3 did not have key access or any other means of non-forcible access to the perimeter gate surrounding the PSP at issue, and RFC_URE5's records of Employee 3 indicate that Employee 3 never attempted to access the PSP during the violation.	30 days after Employee 1 had access to the PSP without a PRA.	The date on which RFC_URE5 revoked the authorized unescorted physical access rights for Employee 3.	$30,000 (for RFC201000393, RFC201000394, and RFC201000773)	Self-Report	RFC_URE5 revoked access rights to Employees 1, 2, and 3. RFC_URE5 also conducted PRAs for Employees 1, 2 and 3, which identified no issues. Additionally, RFC_URE5 is adding a control to its PSP access request process which will require the requestor to confirm PRA status before submitting a request for access to the PSP.	2/22/2011	6/7/2011	Neither Admits nor Denies	The parent company of RFC_URE5 had a compliance program at the time of the violation which ReliabilityFirst considered a mitigating factor. RFC_URE5 does not have any prior violations of the CIP Reliability Standards. ReliabilityFirst did consider the repetitive nature of the violations addressed within this Settlement Agreement as an aggravating factor in the penalty determination. In considering the instant violations, ReliabilityFirst did not observe any evidence of involvement of the entire holding company system or other affiliates.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001887	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence, WECC determined that WECC_URE1 failed to demonstrate that it had procedures in place for the recognition of sabotage events and for making its operating personnel aware of sabotage events on its facilities and on multi-site sabotage events affecting larger portions of the Interconnection, in violation of CIP-001-1 R1.	CIP-001-1	R1	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity but has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size. WECC determined that although sabotage recognition procedures helps personnel assess the sabotage event and determine further actions, the impact on the BPS from a potential sabotage event at WECC_URE1 would have been very limited because of WECC_URE1's limited size, single interconnection to another entity, and unique supply profile serving that other entity only.	The date on which WECC_URE1 was subject to compliance with CIP-001-1 R1.	The date on which WECC_URE1 documented and implemented its sabotage reporting procedure.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan, covering the violations of CIP-001-1 R1-R4. According to the Mitigation Plan, WECC_URE1 implemented procedures for the recognition of sabotage events and for making its personnel aware of such events on its facilities and of multi-site sabotage affecting larger portions of the Interconnection. WECC_URE1 also implemented procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection, provided its operating personnel with sabotage response guidelines, established contacts with local FBI officials and developed appropriate reporting procedures. WECC_URE1 submitted its sabotage recognition and reporting procedure to WECC as evidence of its Mitigation Plan completion.	8/20/2010	2/8/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001888	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. As a result, WECC determined that WECC_URE1 failed to demonstrate that it had procedures in place for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	CIP-001-1	R2	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size. WECC determined that although notifying other operating systems of possible sabotage events increases the situational awareness of the entities interconnected to the BPS, the impact on the BPS from a potential failure to communicate a sabotage event at WECC_URE1 would have been very limited because of WECC_URE1's limited size and single interconnection to another entity, which minimizes the risk to the BPS.	The date on which WECC_URE1 was subject to compliance with CIP-001-1 R2.	The date on which WECC_URE1 documented and implemented its sabotage reporting procedure.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan, covering the violations of CIP-001-1 R1-R4. According to the Mitigation Plan, WECC_URE1 implemented procedures for the recognition of sabotage events and for making its personnel aware of such events on its facilities and of multi-site sabotage affecting larger portions of the Interconnection. WECC_URE1 also implemented procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection, provided its operating personnel with sabotage response guidelines, established contacts with local FBI officials and developed appropriate reporting procedures. WECC_URE1 submitted its sabotage recognition and reporting procedure to WECC as evidence of its Mitigation Plan completion.	8/20/2010	2/8/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001889	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. As a result, WECC determined that WECC_URE1 failed to provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	CIP-001-1	R3	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size. WECC determined that although a lack of sabotage communication guidelines could delay corrective actions on behalf of the entity, the impact on the BPS from a potential failure of WECC_URE1's personnel to report a sabotage event would have been very limited because of WECC_URE1's limited size and single interconnection to another entity, which minimizes the risk to the BPS.	The date on which WECC_URE1 was subject to compliance with CIP-001-1 R3.	The date on which WECC_URE1 documented and implemented its sabotage reporting procedure.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan, covering the violations of CIP-001-1 R1-R4. According to the Mitigation Plan, WECC_URE1 implemented procedures for the recognition of sabotage events and for making its personnel aware of such events on its facilities and of multi-site sabotage affecting larger portions of the Interconnection. WECC_URE1 also implemented procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection, provided its operating personnel with sabotage response guidelines, established contacts with local FBI officials and developed appropriate reporting procedures. WECC_URE1 submitted its sabotage recognition and reporting procedure to WECC as evidence of its Mitigation Plan completion.	8/20/2010	2/8/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001890	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. As a result, WECC determined that WECC_URE1 failed to establish communications contacts with local FBI officials and to develop reporting procedures.	CIP-001-1	R4	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size. WECC determined that although a lack of reporting procedures to the local FBI could lead to sabotage events being unreported, the impact on the BPS from a potential failure of WECC_URE1's personnel to contact the FBI would have been very limited because of WECC_URE1's limited size and single interconnection to another entity, which minimizes the risk to the BPS.	The date on which WECC_URE1 was subject to compliance with CIP-001-1 R4.	The date on which WECC_URE1 documented and implemented its sabotage reporting procedure.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan, covering the violations of CIP-001-1 R1-R4. According to the Mitigation Plan, WECC_URE1 implemented procedures for the recognition of sabotage events and for making its personnel aware of such events on its facilities and of multi-site sabotage affecting larger portions of the Interconnection. WECC_URE1 also implemented procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection, provided its operating personnel with sabotage response guidelines, established contacts with local FBI officials and developed appropriate reporting procedures. WECC_URE1 submitted its sabotage recognition and reporting procedure to WECC as evidence of its Mitigation Plan completion.	8/20/2010	2/8/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002056	Settlement Agreement	WECC notified WECC_URE1 that WECC was initiating a semi-annual CIP Self-Certification process. WECC_URE1 filed a Self-Certification statement and reported that its compliance status for CIP-002-1 R1-R4 was "Not Started." WECC reviewed WECC_URE1's Self-Certification and determined that WECC_URE1 failed to identify and document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets.	CIP-002-1	R1	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because after WECC_URE1 provided and implemented its RBAM following WECC's audit, it became apparent that WECC_URE1 did not have any Critical Assets or Critical Cyber Assets on its system and, therefore, WECC concluded that there had been no actual risk to the BPS. Also, WECC_URE1's size minimizes the risk to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with CIP-002-1 R1.	The date on which WECC_URE1 documented and implemented its methodology document.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Self-Certification	WECC_URE1 submitted a Mitigation Plan covering the violations of CIP-002-1 R1-R4. According to the Mitigation Plan, WECC_URE1 developed and implemented a formal Critical Asset Identification Methodology to be applied in identifying Critical Assets and Critical Cyber Assets. WECC_URE1 also will annually update its list of Critical Assets and Critical Cyber Assets. The methodology document submitted as evidence of compliance included documentation of WECC_URE1's application of its methodology for the purpose of assessing whether WECC_URE1 owns, operates, or controls Critical Assets and Critical Cyber Assets as well as the corresponding asset lists and designated senior manager approvals.	11/15/2010	2/2/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002057	Settlement Agreement	WECC notified WECC_URE1 that WECC was initiating a semi-annual CIP Self-Certification process. WECC_URE1 filed a Self-Certification statement and reported that its compliance status for CIP-002-1 R1-R4 was "Not Started." WECC reviewed WECC_URE1's Self-Certification submittal and determined that WECC_URE1failed to develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology (RBAM) required in R1.	CIP-002-1	R2	High	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because after WECC_URE1 provided and implemented its RBAM following WECC's audit, it became apparent that WECC_URE1 did not have any Critical Assets or Critical Cyber Assets on its system and, therefore, WECC concluded that there had been no actual risk to the BPS. Also, WECC_URE1's size minimizes the risk to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with CIP-002-1 R2.	The date on which WECC_URE1 documented and implemented its methodology document, including a list of Critical Assets.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Self-Certification	WECC_URE1 submitted a Mitigation Plan covering the violations of CIP-002-1 R1-R4. According to the Mitigation Plan, WECC_URE1 developed and implemented a formal Critical Asset Identification Methodology to be applied in identifying Critical Assets and Critical Cyber Assets. WECC_URE1 also will annually update its list of Critical Assets and Critical Cyber Assets. The methodology document submitted as evidence of compliance included documentation of WECC_URE1's application of its methodology for the purpose of assessing whether WECC_URE1 owns, operates, or controls Critical Assets and Critical Cyber Assets as well as the corresponding asset lists and designated senior manager approvals.	11/15/2010	2/2/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002058	Settlement Agreement	WECC notified WECC_URE1 that WECC was initiating a semi-annual CIP Self-Certification process. WECC_URE1 filed a Self-Certification statement and reported that its compliance status for CIP-002-1 R1-R4 was "Not Started." WECC reviewed WECC_URE1's Self-Certification submittal and determined that WECC_URE1failed to develop a list of its associated Critical Cyber Assets that are essential to the operation of the Critical Assets.	CIP-002-1	R3	High	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because after WECC_URE1 provided and implemented its RBAM following WECC's audit, it became apparent that WECC_URE1 did not have any Critical Assets or Critical Cyber Assets on its system and, therefore, WECC concluded that there had been no actual risk to the BPS. Also, WECC_URE1's size minimizes the risk to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with CIP-002-1 R3.	The date on which WECC_URE1 documented and implemented its methodology document, including a list of associated Critical Cyber Assets.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Self-Certification	WECC_URE1 submitted a Mitigation Plan covering the violations of CIP-002-1 R1-R4. According to the Mitigation Plan, WECC_URE1 developed and implemented a formal Critical Asset Identification Methodology to be applied in identifying Critical Assets and Critical Cyber Assets. WECC_URE1 also will annually update its list of Critical Assets and Critical Cyber Assets. The methodology document submitted as evidence of compliance included documentation of WECC_URE1's application of its methodology for the purpose of assessing whether WECC_URE1 owns, operates, or controls Critical Assets and Critical Cyber Assets as well as the corresponding asset lists and designated senior manager approvals.	11/15/2010	2/2/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002059	Settlement Agreement	WECC notified WECC_URE1 that WECC was initiating a semi-annual CIP Self-Certification process. WECC_URE1 filed a Self-Certification statement and reported that its compliance status for CIP-002-1 R1-R4 was "Not Started." WECC reviewed WECC_URE1's Self-Certification submittal and determined that WECC_URE1failed to have a senior manager or delegate approve annually the list of WECC_URE1's Critical Assets or Critical Cyber Assets.	CIP-002-1	R4	Lower	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because after WECC_URE1 provided and implemented its RBAM following WECC's audit, it became apparent that WECC_URE1 did not have any Critical Assets or Critical Cyber Assets on its system and, therefore, WECC concluded that there had been no actual risk to the BPS. Also, WECC_URE1's size minimizes the risk to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with CIP-002-1 R4.	The date on which WECC_URE1 documented and implemented its methodology document, including senior manager or delegate approval.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Self-Certification	WECC_URE1 submitted a Mitigation Plan covering the violations of CIP-002-1 R1-R4. According to the Mitigation Plan, WECC_URE1 developed and implemented a formal Critical Asset Identification Methodology to be applied in identifying Critical Assets and Critical Cyber Assets. WECC_URE1 also will annually update its list of Critical Assets and Critical Cyber Assets. The methodology document submitted as evidence of compliance included documentation of WECC_URE1's application of its methodology for the purpose of assessing whether WECC_URE1 owns, operates, or controls Critical Assets and Critical Cyber Assets as well as the corresponding asset lists and designated senior manager approvals.	11/15/2010	2/2/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001893	Settlement Agreement	On December 4, 2009, WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC, WECC determined that WECC_URE1 failed to provide evidence that it had documented its Facility Rating Methodology, as required by FAC-008-1 R1.	FAC-008-1	R1	Lower	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because of its limited size and a single interconnection to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with FAC-008-1 R1.	The date on which WECC_URE1 documented its Facility Ratings Methodology.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for FAC-008-1 R1. According to the Mitigation Plan, WECC_URE1 documented a Facility Rating Methodology for facilities and equipment at the WECC_URE1 generating facility, including the generator, transmission conductors, transformers, relay protective devices and terminal equipment. As evidence of compliance, WECC_URE1 submitted its Facility Rating Methodology.	9/8/2010	4/5/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001896	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC on several occasions, WECC determined that WECC_URE1 failed to provide evidence that it had established Ratings for its Facilities that are consistent with its associated Facility Ratings Methodology.	FAC-009-1	R1	Medium	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because of its limited size and a single interconnection to the BPS. WECC_URE1 operates a facility with a small nameplate capacity of less than 30 MW. In addition, the risk was substantially mitigated by the fact that WECC_URE1 has only one interconnection to the BPS. WECC_URE1 sells its entire output to another entity and has no significant impact on the other entity's electricity supply or any other facilities connected to the BPS due to its limited size.	The date on which WECC_URE1 was subject to compliance with FAC-009-1 R1.	The date on which WECC_URE1 documented Facility Ratings consistent with its associated Facility Ratings Methodology.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for FAC-009-1 R1. According to the Mitigation Plan, WECC_URE1 documented Facility Ratings as required by this Standard and submitted to WECC its Facility Rating Methodology spreadsheet as evidence of compliance.	9/8/2010	4/12/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001917	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC on several occasions, WECC determined that WECC_URE1 failed to provide evidence that its operating personnel were familiar with the purpose and limitations of Protection System schemes applied in WECC_URE1's area.	PRC-001-1	R1	High	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 operates a small facility of less than 30 MW, and therefore, an unintended trip or a failure to trip could only impact WECC_URE1's equipment but would not have broader implications on the BPS.	The date on which WECC_URE1 was subject to compliance with PRC-001-1 R1.	The date on which WECC_URE1 implemented appropriate training.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for PRC-001-1 R1 and R3. According to the Mitigation Plan, WECC_URE1 developed and implemented procedures and provided associated training to ensure that its operating personnel are familiar with the purposes and limitations of the Protection Systems applied in WECC_URE1's area. WECC_URE1 also implemented training to ensure that new Protection Systems or changes in the existing Protection Systems are coordinated with all appropriate entities. WECC_URE1 submitted a copy of the relevant procedures and training materials as evidence of compliance.	9/24/2010	11/16/2010	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001919	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC on several occasions, WECC determined that WECC_URE1 failed to provide evidence that it coordinated all new protective systems and all protective system changes with its Transmission Operator and Host Balancing Authority.	PRC-001-1	R3	High	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE1 confirmed that it had not experienced any protective system changes that would require Protection System changes by others, including the Transmission Operator and the Host Balancing Authority. In addition, the risk to the BPS was further mitigated by the limited size of the entity and the fact that it has only one interconnection point with the BPS.	The date on which WECC_URE1 was subject to compliance with PRC-001-1 R3.	The date on which WECC_URE1 implemented appropriate training.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for PRC-001-1 R1 and R3. According to the Mitigation Plan, WECC_URE1 developed and implemented procedures and provided associated training to ensure that its operating personnel are familiar with the purposes and limitations of the Protection Systems applied in WECC_URE1's area. WECC_URE1 also implemented training to ensure that new Protection Systems or changes in the existing Protection Systems are coordinated with all appropriate entities. WECC_URE1 submitted a copy of the relevant procedures and training materials as evidence of compliance.	9/24/2010	11/16/2010	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001922	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC on several occasions, WECC determined that WECC_URE1 failed to provide evidence that it had a Protection System maintenance and testing program for Protection Systems that affect the reliability of the bulk power system (BPS), specifically addressing maintenance and testing intervals and their basis and a summary of maintenance and testing procedures.	PRC-005-1	R1	High	Severe	WECC determined that the violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the BPS because WECC_URE1 had acquired outside technical support to perform Protection System maintenance and testing but the documentation of this maintenance and testing did not completely address all of the elements that comprise its Protection System. The relay devices are documented but WECC determined that additional effort was needed to document maintenance and testing of DC circuitry, station batteries, associated communication equipment and voltage and current sensing devices. In addition, the risk to the BPS was further mitigated by the limited size of the entity and the fact that it has only one interconnection point with the BPS.	The date on which WECC_URE1 was subject to compliance with PRC-005-1 R1.	The date on which WECC_URE1 documented its Protection System maintenance and testing program.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for PRC-005-1 R1 and R2.1. According to the Mitigation Plan, WECC_URE1 developed and implemented a documented Protection System maintenance and testing program (Program). The Program includes maintenance and testing intervals and their basis, and addresses relay protective devices, station batteries, voltage and current sensing devices, associated communication systems and DC control circuitry, as appropriate. The Program also includes a summary of maintenance and testing procedures for all BPS elements that comprise WECC_URE1's generator Protection System. As evidence of compliance, WECC_URE1 submitted a copy of the relevant program documents, a list of Protection System components, the schedule for maintenance and testing and documentation regarding testing and maintenance of its Protection System devices.	8/19/2010	3/22/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.
Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201001923	Settlement Agreement	WECC sent WECC_URE1 a Notice of Off-Site Compliance Audit directing WECC_URE1 to provide evidence demonstrating compliance with the Reliability Standards. WECC_URE1 failed to submit audit evidence following the notice. Subsequently, WECC sent three additional notices, directing WECC_URE1 to submit the requested evidence but the entity did not respond. Based on WECC_URE1's failure to submit audit evidence as requested by WECC on several occasions, WECC determined that WECC_URE1 failed to provide evidence of its Protection System maintenance and testing program and the implementation of that program, including evidence that the Protection Systems were maintained and tested within the defined intervals, and the date each Protection System was last tested or maintained.	PRC-005-1	R2.1	High	Severe	WECC determined that the violation did not pose serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS) because although WECC_URE1 did not provide evidence that its Protection Systems were maintained and tested within defined intervals, WECC_URE1 subsequently provided evidence, as part of its Mitigation Plan completion, demonstrating that its Protection System devices had been tested and maintained.	The date on which WECC_URE1 was subject to compliance with PRC-005-1 R2.	The date on which WECC_URE1 documented testing and maintenance of its Protection System devices.	$90,000 (for WECC201001887, WECC201001888, WECC201001889, WECC201001890, WECC201002056, WECC201002057, WECC201002058, WECC201002059, WECC201001893, WECC201001896, WECC201001917, WECC201001919, WECC201001922, WECC201001923)	Off-Site Compliance Audit	WECC_URE1 submitted a Mitigation Plan for PRC-005-1 R1 and R2.1. According to the Mitigation Plan, WECC_URE1 developed and implemented a documented Protection System maintenance and testing program (Program). The Program includes maintenance and testing intervals and their basis, and addresses relay protective devices, station batteries, voltage and current sensing devices, associated communication systems and DC control circuitry, as appropriate. The Program also includes a summary of maintenance and testing procedures for all BPS elements that comprise WECC_URE1's generator Protection System. As evidence of compliance, WECC_URE1 submitted a copy of the relevant program documents, a list of Protection System components, the schedule for maintenance and testing and documentation regarding testing and maintenance of its Protection System devices.	8/19/2010	3/22/2011	Agree and stipulate to the facts.	Mitigating Factors: WECC_URE1 developed and implemented an internal compliance program (ICP), designed to govern WECC_URE1's future compliance efforts. Aggravating Factors: 1) WECC_URE1 was not cooperative with WECC and did not demonstrate a culture of compliance during the compliance auditing process, and 2) WECC_URE1 did not timely complete its mandatory Self-Certification.

Attachment A-2
September 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (CIP and NON-CIP)

Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation (For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, or confirmed violation.)	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002367	Notice of Confirmed Violation	On January 26, 2010, WECC_URE2 submitted Self-Reports to WECC concerning violations of CIP-007-1 R3 and R6. On November 22, 2010, a WECC subject matter expert (SME) conducted an interview with WECC_URE2 personnel, and determined that WECC_URE2's CIP-007 Self-Reports involved one server used for controlling physical access (doors) at three Physical Security Perimeters (PSPs). Then, the SME determined that CIP-007 does not cover such devices. Therefore, on December 30, 2010, WECC_URE2 replaced its CIP-007 Self-Reports with a single Self-Report addressing a violation of CIP-006-1 R1.8. In its new Self-Report, WECC_URE2 clarified that the server is used for physical access and monitoring its primary control center. A WECC SME reviewed WECC_URE2's CIP-006-1 R1 Self-Report, and determined WECC_URE2 did not assess available security patches for the server and did not review the server's system event logs. WECC determined that WECC_URE2's failure to assess the available security patches or review the server's system event logs did not afford the server the protective measures specified in CIP-007.	CIP-006-1	R1	Medium	Moderate	WECC determined that the violation of CIP-006-1 R1 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2 stated that the access control and monitoring assets to its primary control center, including the server at issue, were in a facility that logged, detected, and alarmed for unauthorized physical and electronic access.	The date on which WECC_URE2 was subject to compliance with CIP-006-1 R1.	The date on which WECC_URE2 implemented an appropriate patch management system and enabled logging.	$20,400 (for WECC201002367, WECC201002323, and WECC201002324)	Self-Report	WECC_URE2 combined the update service of the cyber systems to the current server updated services database to better manage, audit, and report security patch management. WECC_URE2 enabled logging and is performing weekly log reviews as defined in its CIP-007 R6 cyber security event procedure.	3/1/2010	7/21/2011	Does Not Contest	WECC_URE2 had a documented internal compliance program (ICP) at the time of the violation that WECC considered as a mitigating factor in determining the penalty. WECC determined that the WECC_URE2 ICP has been reviewed and approved by an Authorized Entity Officer or equivalent, is fully documented, reviewed and approved by an Authorized Entity Officer or equivalent, and has an oversight position identified and staffed.
Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002323	Notice of Confirmed Violation	WECC notified WECC_URE2 that WECC was initiating the semi-annual CIP Self-Certification process for the year ending 2009. On January 28, 2010, WECC_URE2 submitted a Self-Report to WECC concerning a violation of CIP-006-1 R6 due to WECC_URE2's failure to implement a maintenance and testing program to ensure the functionality of WECC_URE2's physical security systems. Although WECC_URE2 self-reported this violation, because WECC_URE2 self-reported during the Self-Certification submission period, WECC classified the discovery method for this violation as Self-Certification. On November 22, 2010, a WECC SME conducted an interview with WECC_URE2 personnel where WECC_URE2 clarified that it did not perform baseline testing prior to or on its mandatory compliance date. The SME determined that WECC_URE2 did not conduct testing on its system, which is comprised of a server, workstations, card readers, and door readers in order to provide locking and opening controls at access points. In addition, WECC_URE2's system provides alarms and alerts to a centralized database, and is associated with three Physical Security Perimeters (PSPs), including WECC_URE2's (1) data center, (2) primary control center, and (3) back-up control center. WECC determined, by not performing baseline testing, WECC_URE2 failed to implement a maintenance and testing program to ensure that WECC_URE2 physical security systems under CIP-006-1 R2-R4 function properly.	CIP-006-1	R6	Medium	Moderate	WECC determined that the violation of CIP-006-1 R6 posed a moderate risk to the reliability of the bulk power system (BPS) because WECC_URE2 failed to implement a maintenance and testing program for the physical security systems for three PSPs, including the primary control center, backup control center and a data center. The physical security system was used for access control, monitoring and logging at these PSPs, and the failure to implement the maintenance and testing program could allow physical security systems to malfunction and potential unauthorized access to the PSPs. WECC determined, however, that the violation did not pose a serious or substantial risk to the BPS because the facilities had physical and electronic access logging, were continuously monitored including video monitoring of access points and weekly log reviews were conducted by WECC_URE2. In addition, WECC_URE2 has an incident response plan, and hardware alerts for a physical security device failure.	The date on which WECC_URE2 was subject to compliance with CIP-006-1 R6.	The date on which WECC_URE2 performed and documented baseline testing.	$20,400 (for WECC201002367, WECC201002323, and WECC201002324)	Self-Certification	WECC_URE2 performed a test in accordance with its CIP physical security maintenance test program in order to provide evidence to establish a documented baseline.	2/10/2010	12/15/2010	Does Not Contest	WECC_URE2 had a documented internal compliance program (ICP) at the time of the violation that WECC considered as a mitigating factor in determining the penalty. WECC determined that the WECC_URE2 ICP has been reviewed and approved by an Authorized Entity Officer or equivalent, is fully documented, reviewed and approved by an Authorized Entity Officer or equivalent, and has an oversight position identified and staffed.
Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002324	Notice of Confirmed Violation	On October 21, 2010, WECC_URE2 discovered a possible violation of CIP-007-1 R5. Then, on November 10, 2010, WECC_URE2 submitted a Self-Report to WECC concerning a violation of CIP-007-1 R5 due to WECC_URE2's failure to document procedural controls that enforce access authentication and accountability for all user activity for 31 devices, including switches, firewalls, and servers. On November 22, 2010, a WECC SME conducted an interview with WECC_URE2 personnel who clarified information from its Self-Report stating that where WECC_URE2 could not use automated software to enforce password complexity, WECC_URE2 has a procedure for doing annual password changes in manual fashion. WECC_URE2's procedure calls for password cracking tools to validate if a password met the complexity requirements outlined in CIP-007 R5.3. The SME determined that after WECC_URE2 installed such password cracking/validation tools pursuant to WECC_URE2's account management procedure, WECC_URE2's test machines crashed. Therefore, WECC_URE2 created a process to maintain password complexity through accountability and witness documentation of password changes and complexity based on the requirements. Both WECC_URE2 and the SME determined that WECC_URE2 had to institute this accountability and witness process on 31 devices, including switches, firewalls, and servers located in WECC_URE2's control center and data center, that were Critical Cyber Assets or Cyber Assets within the Electronic Security Perimeter. Nevertheless, WECC determined WECC_URE2 did not document the manual process associated with the 31 devices.	CIP-007-1	R5	Lower	Moderate	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because while WECC_URE2 did not update its documented account management procedures to reflect procedural controls, WECC_URE2 did in fact follow its manual process of annually changing passwords with manual authentication and witness controls. In addition, WECC_URE2 did enforce authentication and accountability of all user activity for systems access by establishing and implementing technical controls as required by the standard.	The date on which WECC_URE2 was subject to compliance with CIP-007-1 R5.	TBD	$20,400 (for WECC201002367, WECC201002323, and WECC201002324)	Self-Report	WECC_URE2 rewrote procedures to address manual processes that were occurring internally, and drafted additional procedures dealing with default, administrative and shared accounts to assist in sustaining compliance. WECC_URE2 completed a scheduled upgrade to its Energy Management System (EMS) to eliminate system dependencies on shared accounts. WECC_URE2 changed its accounts to the normal password expiration required by CIP-007 R5 password management procedure. WECC_URE2 documented previously undocumented user IDs as shared accounts and the domain automated password complexity and aging was enabled for these accounts as well. WECC_URE2 provided additional training of its CIP-007 R5 shared account management procedure in order to utilize automated task management solutions to schedule and escalate tasks. WECC_URE2 began adhering to and follow its existing procedures and tasks associated to changing shared accounts passwords when employees with access retire, leave employment or change job responsibilities. WECC_URE2 began adhering to and following its existing procedures and tasks associated to changing accounts passwords. WECC_URE2 generated unique user IDs for management personnel and follow complexity and aging requirements set forth within the procedure. WECC_URE2 began utilizing task management programs to alert the responsible personnel of specific tasks needing to be performed. WECC_URE2 began issuing, tracking and escalating tasks based on the relative due date of the task. WECC_URE2 began revising its CIP-007 R1 testing procedure to better align with test process and other standard requirement procedures to prevent or minimize overlooked areas. WECC_URE2 began revising its password procedures to better align the internal process to prevent or minimize adverse effects on system operations while maintaining compliance. WECC_URE2 began adhering to the procedures as well as automated task management, escalation and auditing in order to assist in sustaining future compliance.	12/30/2011 (approved date)	TBD	Does Not Contest	WECC_URE2 had a documented internal compliance program (ICP) at the time of the violation that WECC considered as a mitigating factor in determining the penalty. WECC determined that the WECC_URE2 ICP has been reviewed and approved by an Authorized Entity Officer or equivalent, is fully documented, reviewed and approved by an Authorized Entity Officer or equivalent, and has an oversight position identified and staffed. WECC determined that WECC_URE2's prior violations of CIP-007-1 R1 and CIP-007-1 R6 should not serve as a basis for aggravating the penalty because the instant violation is sufficiently distinct due to the unique differences between Critical Cyber Assets (protected in accordance with CIP-007).

Document Content(s)

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900228	Settlement Agreement	The entity as a Transmission Operator failed to include applicable elements in its emergency operations plan, specifically, notification of appropriate government agencies and notification to operating entities.	EOP-001-0	R5	Medium	Moderate (2 out of 15, 87%)	This violation posed a minimal risk and did not pose serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC had a standard practice of communicating with appropriate parties during normal and emergency situations even though it had not documented the process in its emergency plan.	6/18/2007	11/30/2009	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity developed and implemented a new communication procedure as part of its Emergency Plan, that addressed notification of appropriate government agencies and notification to operating entities.	11/30/2009	1/8/2010	Neither Admits nor Denies
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900229	Settlement Agreement	The entity as a Transmission Operator had not coordinated its manual load shedding plan with other interconnected Transmission Operators and Balancing Authorities.	EOP-003-1	R3	High	Severe	This violation posed a minimal risk and did not pose serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC had developed a manual load shedding plan and had procedures in place to coordinate the implementation of its plan with its Balancing Authority.	6/18/2007	10/30/2009	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity provided its manual load shedding plan to other interconnected Transmission Operators for review to ensure the plan would coordinate with the entities.	10/30/2009 (evidence indicates completion of milestone 2 on 10/30/2009; however, the Mitigation Plan, Certification, and auditor all indicate 10/31/2009)	1/8/2010	Neither Admits nor Denies
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900230	Settlement Agreement	The entity's system restoration plan did not include elements 6 and 7 of EOP-005-1 Attachment 1 for: 6. Procedures for simulating and where practical, actually testing and verifying the plans resources and procedures. 7. Retaining documentation of personnel training records that operating personnel have been trained annually in the implementation of the plan and have participated in restoration exercises.	EOP-005-1	R1	Medium	Lower (2 out of 9; 78%)	This violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC's personnel routinely participated in FRCC's annual system operator training workshops and BPS restoration drills of its Balancing Authority.	6/18/2007	3/15/2010	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity revised its restoration plan to include elements 6 and 7 of EOP-005-1 Attachment 1. It also developed restoration simulations and provided training to its operating personnel.	3/15/2010	5/5/2010	Neither Admits nor Denies
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900231	Settlement Agreement	The entity did not train its operating personnel in the implementation of its restoration plan for 2008 and 2009.	EOP-005-1	R6	High	Severe	This violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC's personnel routinely participated in FRCC's annual system operator training workshops and BPS restoration drills of its Balancing Authority.	1/1/2008	3/12/2010	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity provided training to its operating personnel in the implementation of its restoration plan.	3/12/2010 (evidence indicates completion of training on 3/12/2010 although the Mitigation Plan and auditor indicate 3/15/2010)	5/5/2010	Neither Admits nor Denies

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900233	Settlement Agreement	The entity did not maintain and publish its facility connection requirements consistent with NERC Reliability Standards, the applicable Regional Reliability Organization/Regional Entity, subregional, Power Pool, and individual Transmission Owner planning criteria and facility connection requirements for generation facilities, transmission facilities, and end-user facilities.	FAC-001-0	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC's *FAC-001 Policy/Procedure* dated 1/1/2007 describes the process for establishing specific facility connection requirements for LCEC's BPS. The procedures are based upon an agreement with its Balancing Authority and its interconnected entity.	6/18/2007	11/4/2009	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity created and published a new facility connection requirements document consistent with the NERC Requirement.	11/4/2009	1/20/2010	Neither Admits nor Denies
FRCC	Lee County Electric Cooperative, Inc (LCEC)	NCR00045	FRCC200900244	Settlement Agreement	The entity did not provide sufficient evidence to demonstrate that it jointly developed formal policies and procedures for monitoring and controlling voltage levels and Mega Volt Ampere Reactive (Mvar) flows with its neighboring Transmission Operators.	VAR-001-1	R1	High	High	This violation posed a minimal risk and did not pose a serious and substantial risk to the reliability of the bulk power system (BPS) because LCEC had ensured that formal policies and procedures were developed, maintained and implemented for monitoring and controlling voltage levels in Mvar flows within its individual areas.	6/18/2007	11/2/2009	$30,000 (for FRCC200900228, FRCC200900229, FRCC200900230, FRCC200900231, FRCC200900233, and FRCC200900244)	Audit (8/28/2009)	The entity contacted its neighboring Transmission Operators and requested a review of its voltage and reactive control policies and procedures. The neighboring Transmission Operators provided a response back to the entity the policies and procedures for monitoring and controlling voltage levels and Mvar flows was adequate.	11/2/2009	1/20/2010	Neither Admits nor Denies
MRO	LSP-Cottage Grove, LP (LSP-CGLP)	NCR10022	MRO201100255	Notice of Confirmed Violation	On January 13, 2011, LSP-CGLP self-reported noncompliant with Reliability Standard PRC-005-1 R1 because its Protection System maintenance and testing program did not address maintenance and testing intervals and basis, and failed to contain a summary of maintenance and testing procedures for voltage and current sensing devices (VCSDs) and DC control circuitry. Upon reviewing the self-report and LSP-CGLP's Protection System maintenance and testing program, MRO confirmed that the program failed to address maintenance and testing intervals and their basis, and failed to contain a summary of maintenance and testing procedures for VCSDs and DC control circuitry. Therefore, LSP-CGLP failed to maintain a Protection System maintenance and testing program as required by PRC-005-1 R1.	PRC-005-1	R1	High	Lower	MRO determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although LSP-CGLP's Protection System maintenance and testing program failed to address maintenance and testing intervals and their respective basis for VCSDs and DC control circuitry, LSP-CGLP functionally tested all DC control circuitry up to the trip coil on the associated circuit breaker, and VCSDs were tested during equipment commissioning and are continuously monitored. Additionally, during the comprehensive review of protection system components, LSP-CGLP did not identify any performance issues with VCSDs or DC control circuitry, which were verified as part of LSP-CGLP's mitigation plan.	7/11/2007	3/31/2011	$0	Self-Report	LSP-CGLP's Protection System maintenance and testing program was revised to include a summary of maintenance and testing procedures, and maintenance and testing intervals and their respective basis for voltage and current sensing devices (VCSDs) and DC control circuitry.	3/31/2011	4/7/2011	Does not contest

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
MRO	NorthWestern Energy (NWE)	NCR01021	MRO201000198	Notice of Confirmed Violation	On July 22, 2010, NWE self-reported a violation of PRC-008-0 R2. NWE discovered this violation by conducting an annual internal compliance review. Upon receiving the report, MRO requested that NWE perform a full inventory of its Under Frequency Load Shedding (UFLS) equipment, and provide all maintenance and testing records for its UFLS equipment. Upon performing the review, NWE reported that it has 68 UFLS devices. Of the 68 devices, NWE performed maintenance of 99% of the devices and performed testing of 41 devices in accordance with its UFLS program, or approximately 60%. Therefore, NWE performed UFLS maintenance and testing for approximately 79% of its UFLS equipment.	PRC-008-0	R2	Medium	Lower	MRO determined that this violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NWE performed maintenance on 99% of its UFLS equipment and tested 60% of its UFLS equipment. Additionally, NWE's UFLS is based on the 2010 Summer Peak System Load model and sheds 102.4 MW of 322.20 MW of modeled load. This is not done directly on the 115 kV system. Instead, it is accomplished on 69 kV, 34.5 kV, and 4.16 kV circuits. Therefore, MRO determined that this violation posed a minimal risk to the BPS because of the size of the load.	6/18/2007	1/14/2011	$0	Self-Report	NWE performed the following actions to mitigate the violation: (1) updated its UFLS maintenance and testing program to include potential transformers, batteries and DC circuitry; (2) developed a full inventory of UFLS equipment to determine the equipment that had not been maintained and tested; and (3) scheduled, performed and documented the testing required on additional UFLS equipment identified in the review process.	1/14/2011	2/7/2011	Admits
NPCC	Mirant Canal	NCR07146	NPCC201000130	NOCV	At 06:23 am on Sunday December 20, 2009 the Transmission Operator (TOP) experienced trouble on the 121 line Auto Transformer resulting in a loss of reserve station service to Unit #1. At that time, Canal unit 1 was unavailable for startup. The plant supervisor contacted NSTAR bulk power and arranged for the TOP to dispatch a crew to determine the problem in the switch yard. A substantial snow storm made this job much more difficult than usual and the plant did not inform the Mirant real time desk of the change in unit status until 10:55 am. Around that time the Balancing Authority was notified of the unavailability of Unit 1 but it was approximately 4 ½ hours after the outage had started.	TOP-002-2a	14.1	Medium	Severe	NPCC Enforcement determined that the alleged violation posed a minimal and did not pose serious or substantial risk to the bulk power system (BPS) because during the period that Unit#1 was unavailable it was on a reserve shutdown. Also, Unit#1 was not requested to come on line by the Balancing Authority and Transmission Operator.	1/20/2009	1/20/2009	$0	Self-Certification	1. A "Re-affirmation of Notification Requirements pertaining to TOP-002-2" Requirement 14 was reviewed with employees responsible for making such notifications when changes in capability of the generator occur. 2. Awareness posters were installed in the Control Room to remind operators of the requirement to make notifications whenever there is a change in generator capability.	1/25/2010	6/3/2011	Does not Contest
NPCC	Mt. Tom Generating Co. LLC	NCR10050	NPCC201000167	NOCV	During an internal audit of NERC Compliance, it was determined that the Station's Protection System devices (specifically protective relays) were not maintained and tested within the intervals defined in internal procedure MP-2006-01, Relay Protection System Maintenance and Testing, Revision 0 dated November 29, 2006. This revision of the procedure prescribed that the electromechanical protective relays systems at the Station be maintained and tested on a two year basis. Maintenance and testing was performed between May 1 and May 4, 2006. In accordance with the procedural requirements, testing should have been performed in May 2008. However, maintenance and testing was not completed until the period May 18 through June 3, 2009, trip tests were completed on October 31, 2009, and Current Transformer (CT) and Potential Transformer (PT) testing was completed on May 6, 2011.	PRC-005-1	2.1, 2.2	High	Severe	NPCC determined that the violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because all relay systems were within the correct specifications and operated properly with the exception of the generator negative phase sequence relay which was replaced and tested satisfactorily on October 31, 2009. Also, Mt. Toms relay maintenance program requires testing on a 2 year basis which is more frequent than industry standards.	1/4/2008	5/6/2011	$5,000.00	Self-Report	1. Mt. Tom completed relay testing on June 3, 2009. 2. Mt. Tom completed station trip testing on October 31, 2009 3. Mt. Tom completed CT and PT testing on May 6, 2011	5/6/2011	6/3/2011	Does not Contest

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	Dynegy Inc. (Dynegy)	NCR00200	SERC200900323	Notice of Confirmed Violation	Dynegy, as a Generator Operator, was in violation of VAR-002-1a R1 because it failed to operate a generator in the automatic voltage control mode and did not notify its Transmission Operator as required by the Standard on three separate instances, each of which was less than 30 seconds. Two of the instances occurred on November 2, 2008, and one occurred on February 15, 2009. The two durations on November 2 were for 4 seconds and for 29 seconds. The duration on February 15 was for 7 seconds. No notification was made to the TO. SERC recognizes that previous violations of R2 were addressed in a settlement agreement with Dynegy in NP09-000. However, the facts and circumstances are different and the Mitigation Plan could not have addressed and prevented the current violations.	VAR-002-1a	R1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The total duration for the three events was less than one minute; 2. The generating unit maintained its voltage schedule within the bounds of the Interconnection and operating agreement applicable to the unit; 3. The incident involved a single unit; and 4. The Transmission Operator did not communicate any directives or report any reliability problems or issues to the generation site during the time period of the violation.	11/2/2008	2/15/2009	$5,000 (for SERC200900323 and SERC200900324)	Self- Report	Dynegy completed the following: 1. Provided its Houston Control Center (HCC) operating personnel with e-mails concerning AVR issues and reminding them of the need to contact the Transmission Operator of an AVR status change; 2. Revised its *Generation Operations Procedure* and *Generation Operations Policy* to clarify that all AVR status changes, regardless of duration, shall be reported to the Transmission Operator; and 3. Conducted formal training for HCC operating personnel regarding this standard as well as *Generation Operations Procedure* and *Generation Operations Policy*.	11/4/2009	4/18/2010	Admits
SERC	Dynegy Inc. (Dynegy)	NCR00200	SERC200900324	Notice of Confirmed Violation	Dynegy, as Generator Operator, was in violation of VAR-002-1a R3 because on November 2, 2008 it did not notify its Transmission Operator of the status change in the Automatic Voltage Regulator (AVR) operation at Wood River Unit 5 within the 30 minute requirement of the Standard on three separate instances. Two of the instances occurred on November 2, 2008, and one occurred on February 15, 2009. The duration of this violation is less than one day. SERC recognizes that previous violations of R2 were addressed in a settlement agreement with Dynegy in NP09-000. However, the facts and circumstances of the current violation are different and the Mitigation Plan could not have addressed and prevented the current violations.	VAR-002-1a	R3	Medium	High	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The total duration for the three events was less than one minute; 2. The generating unit maintained its voltage schedule within the bounds of the Interconnection and operating agreement applicable to the unit; 3. The incident involved a single unit; and 4. The Transmission Operator did not communicate any directives or report any reliability problems or issues to the generation site during the time period of the violation.	11/2/2008	2/15/2009	$5,000 (for SERC200900323 and SERC200900324)	Self- Report	Dynegy completed the following: 1. Provided its Houston Control Center (HCC) operating personnel with e-mails concerning AVR issues and reminding them of the need to contact the Transmission Operator of an AVR status change; 2. Revised its *Generation Operations Procedure* and *Generation Operations Policy* to clarify that all AVR status changes, regardless of duration, shall be reported to the Transmission Operator; and 3. Conducted formal training for HCC operating personnel regarding this standard as well as *Generation Operations Procedure* and *Generation Operations Policy*.	11/4/2009	4/18/2010	Admits
SERC	Progress Energy Carolinas (PEC)	NCR01298	SERC200900327	Notice of Confirmed Violation	PEC, as a Purchase-Selling Entity, violated INT-001-3 R1 because it failed to submit Dynamic Schedules to its Interchange Authority on four separate instances between October 2007 and September 2009. After discovering the missing e-tag in September 2009, PEC searched through its past records and found three other instances of missing e-tags.	INT-001-3	R1	Lower	Moderate	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The contract resources for the wholesale customer are dynamically scheduled based on metered load so the dynamic schedule always matches the wholesale customer's load, and the other interchange transaction information was agreed upon prior to the Dynamic Schedule implementation; and 2. PEC's Balancing Authority includes the wholesale customer hourly integrated Dynamic Schedule in its schedule checkout process. This Dynamic Schedule accurately served the wholesale customer load without an energy imbalance or inadvertent energy despite the absence of a tag during those periods.	10/1/2007	9/14/2009	$0	Self-Report	PEC completed the following actions: 1. As soon as the missing tag was discovered, PEC posted the Dynamic Schedule for the remainder of the month of September 2009; 2. Performed an investigation of all long term contracts for adherence to NERC tagging standards; 3. Established an improved work process with redundancy and verification; 4. Established and implemented a mandatory periodic Reliability Standards training; and 5. Developed and implemented an internal procedure covering the creation, verification and submittal of e-tags.	12/31/2009	3/15/2010	Admits

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	Progress Energy Carolinas (PEC)	NCR01298	SERC201000441	Notice of Confirmed Violation	PEC, as a Purchasing-Selling Entity, violated INT-004-2 R2 for failure to update its Dynamic Transfer tags after exceeding the thresholds, as required by the Standard, for 216 out of 17,328 hours.	INT-004-2	R2	Lower	Lower	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The size of the Dynamic Transfers (800 MW) is small relative to PEC's system load of approximately 13,000 MW and the most extreme deviation identified was 547 MW (595 MW scheduled and 48 MW delivered); 2. The actual transfers were within the limits established for the reservation of firm transmission; and 3. None of the excursions from the scheduled energy profile resulted in the issuance of transmission loading relief directives.	5/20/2008	8/2/2010	$0	Self-Report	PEC completed the following actions: 1. Implemented a new algorithm for the automated tag adjustment process that re-forecasts the Dynamic Schedule and adjusts the tag when the deviation approaches or exceeds the limits of the standard; 2. Issued a standing order to make staff aware of the tag policy for dynamic scheduling and modification for future tags; 3. Monitored the new automated tag adjustment process and issued a standing order implementing the improved algorithm for automated tag adjustments; and 4. Retrained all operators and scheduling personnel within PEC on Dynamic Schedule tagging.	8/2/2010	1/24/2011	Admits
SERC	Town of Stantonsburg (Stantonsburg)	NCR01349	SERC201100774	Notice of Confirmed Violation	Stantonsburg, as a Distribution Provider with an Under Frequency Load Shedding (UFLS) program, was in violation of PRC-008-0 R1 for failing to have a UFLS equipment maintenance and testing program in place.	PRC-008-0	R1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Stantonsburg is a minimal size utility of 6.1 MW with 1,095 residential customers and 80 commercial consumers and owns no BPS facilities. Stantonsburg's contribution to underfrequency load shed pursuant to the SERC regional criteria (30% of peak load) is 2 MW. Because Stantonsburg is connected radially and of minimal size, it should have little impact on the BPS if an underfrequency event had occurred and its UFLS equipment had not responded as planned; and 2. Stantonsburg provided evidence that it was testing its UFLS equipment.	6/18/2007	1/19/2011	$0	Self-Report	Stantonsburg developed a UFLS procedure that documents the exact location, the identification, the dates of installation, and sets the schedule for the testing and maintenance of its UFLS equipment.	1/19/2011	7/6/2011	Admits
SERC	City of Camden (Camden)	NCR01195	SERC201000557	Notice of Confirmed Violation	Camden, as a Load-Serving Entity, was in violation of CIP-001-1 R1 for failing to have procedures for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection.	CIP-001-1	R1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Camden is a minimal size utility of 52 MW serving 8,046 residential and 1,316 commercial customers with approximately 650 miles of distribution lines at 12 kV. Camden does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS should be recognized and reported by the TO/TOP.	6/18/2007	8/13/2010	$0	On-site audit	Camden performed the following: 1. Added the definition of sabotage to its *Sabotage Reporting and Restoration Procedure* ; and 2. Added language to the procedure that prompts Camden to call its electric reliability contacts when sabotage is suspected.	8/13/2010	6/17/2011	Admits

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	City of Camden (Camden)	NCR01195	SERC201000558	Notice of Confirmed Violation	Camden, as a Load-Serving Entity, was in violation of CIP-001-1 R2 for failing to have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	CIP-001-1	R2	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Camden is a minimal size utility of 52 MW serving 8,046 residential and 1,316 commercial customers with approximately 650 miles of distribution lines at 12 kV. Camden does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS should be recognized and reported by the TO/TOP.	6/18/2007	8/13/2010	$0	On-site Audit	Camden performed the following: 1. Added the definition of sabotage to its *Sabotage Reporting and Restoration Procedure* ; and 2. Added language to the procedure that prompts Camden to call its electric reliability contacts when sabotage is suspected.	8/13/2010	6/17/2011	Admits
SERC	City of Camden (Camden)	NCR01195	SERC201000559	Notice of Confirmed Violation	Camden, as a Distribution Provider with an Under Frequency Load Shedding (UFLS) program, violated PRC-008-0 R1 for failing to have a UFLS equipment maintenance and testing program. Camden did not have a written procedure addressing UFLS equipment identification or a schedule for UFLS equipment testing and maintenance. However, pursuant to an agreement between Camden and Camden's Transmission Owner/Transmission Operator (TO/TOP), the TO/TOP was performing monthly visual inspections of Camden's substations since June 2007.	PRC-008-0	R1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Camden is a minimal size utility of 52 MW serving 8,046 residential and 1,316 commercial customers with approximately 650 miles of distribution lines at 12 kV. Because Camden is connected radially and of minimal size, it should have little impact on the BPS if an underfrequency event had occurred; 2. Camden's TO/TOP has its own Protection System. In addition, Camden owns protective relaying to protect Camden-owned equipment on the Camden side of the delivery point. There is no interaction between the Camden-owned Protection System and the TO/TOP Protection System. Because of this configuration, events on the Camden electric system should not affect the BPS; and 3. Camden's TO/TOP has inspected Camden's substations including the UFLS devices monthly since June 2007, and a third party contractor has been performing maintenance on Camden's substation equipment, which should include the UFLS devices, since 2007.	6/18/2007	4/21/2010	$0	On-site Audit	Camden completed the following actions: 1. Added UFLS components to the monthly inspection checklist in order to show that they are being inspected. 2. Created a relay inspection checklist; and 3. Developed instructions addressing the maintenance and document retention policy that was added to the UFLS maintenance and testing program.	4/21/2011	5/25/2011	Admits

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	City of Camden (Camden)	NCR01195	SERC201000560	Notice of Confirmed Violation	Camden, as a Distribution Provider with an Under Frequency Load Shedding (UFLS) program, was in violation of PRC-008-0 R2 for failing to provide evidence that its UFLS maintenance and testing program was properly implemented. While Camden's Transmission Owner/Transmission Operator (TO/TOP) performed monthly visual inspections, Camden was unable to provide evidence showing what, if any, actual maintenance and testing had been performed on the under frequency relays.	PRC-008-0	R2	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Camden is a minimal size utility of 52 MW serving 8,046 residential and 1,316 commercial customers with approximately 650 miles of distribution lines at 12 kV. Because Camden is connected radially and of minimal size, it should have little impact on the BPS if an underfrequency event had occurred; 2. Camden's TO/TOP has its own Protection System. In addition, Camden owns protective relaying to protect Camden-owned equipment on the Camden side of the delivery point. There is no interaction between the Camden-owned Protection System and the TO/TOP Protection System. Because of this configuration, events on the Camden electric system should not affect the BPS; and 3. Camden's TO/TOP has inspected Camden's substations including the UFLS devices monthly since June 2007, and a third party contractor has been performing maintenance on Camden's substation equipment, which should include the UFLS devices, since 2007.	6/18/2007	4/21/2011	$0	On-site Audit	Camden completed the following actions: 1. Added UFLS components to the monthly inspection checklist in order to show that they are being inspected; 2. Created a relay inspection checklist; and 3. Developed instructions addressing the maintenance and document retention policy that was added to the UFLS maintenance and testing program.	4/21/2011	5/25/2011	Admits
SERC	Cogentrix Virginia Leasing Corp (Cogentrix)	NCR01206	SERC201000579	Notice of Confirmed Violation	Cogentrix, as an owner of a generation Protection System, violated PRC-005-1 R1 for failing to have a procedure that included associated communication systems or maintenance and testing intervals for its Protection System devices, although all devices were being maintained and tested.	PRC-005-1	R1	High	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. The SERC audit team had no findings regarding PRC-005-1 R2. Prior to Cogentrix developing a procedure that met the requirements of the Standard, its Protection System devices were being tested and maintained based on either the manufacturer's recommendations or intervals that are within acceptable industry practice (5 years or less for all devices). Cogentrix does not have any associated communication systems.	6/18/2007	11/27/2007	$0	On-site Audit	Cogentrix revised its *Summary of Maintenance and Testing Procedure* document to address each Protection System device and included the maintenance and testing intervals, their basis, and the summary of the maintenance and testing procedures.	11/27/2007	6/9/2011	Admits
SPP RE /RFC	American Electric Power Services Corp. As Agent For Public Svc. Co. Of Oklahoma & SW Ele Pwr Co. / American Electric Power Service Corporation as agent for Appalachian Power Company, Columbus Southern Power Company, Indiana Michigan Power Company, Kentucky Power Company, Kingsport Power Company, Ohio Power Company, and Wheeling Power Company (AEP)	NCR01056 NCR00682	SPP200900151 RFC200900322	Settlement Agreement	During an October 29, 2009 joint SPP RE / Reliability*First* compliance audit, the Regional Entities concluded that AEP's generator Facility Ratings Methodology did not include terminal equipment (specifically, disconnect switches) and relay protective devices.	FAC-008-1	R1.2.1	Medium	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS). The disconnect switches were considered in the evaluation of the generator Facility Ratings, and AEP's design practice precludes using relay protective devices to establish the Rating of its generation Facilities. Moreover, AEP's identification of the most limiting factor of the generation Facilities did not change after the previously excluded devices were included in AEP's generator Facility Ratings Methodology.	10/29/2009	12/31/2009	$8,000 (for SPP200900151 / RFC200900322)	Compliance Audit	AEP revised its generator Facility Ratings Methodology to include terminal equipment and relay protective devices.	12/31/2009	3/18/2010	Neither Admits nor Denies

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
Texas RE	Bosque Power Company, LLC	NCR10247	TRE200900134	Settlement Agreement	The previous generation Protection System testing and maintenance procedure used by Bosque did not address all sub-requirements listed in PRC-005-1 R1. The program was missing testing intervals for instrument transformers (CT/PTs), DC circuitry, communication systems and a technical basis for intervals.	PRC-005-1	1	High	High	This violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system because actual testing on Protection System devices was being performed within industry accepted intervals. Moreover, a Protection System program existed and addressed the summary of testing procedures for all protection devices. The explicit listing of testing intervals and basis was missing.	5/1/2008	5/6/2011	$13,000 (for TRE200900134 and TRE200900135)	Self-Report	Bosque revised its Protection System maintenance and testing procedure as of May 6, 2011 to include a specific task to ensure that none of the required test are overlooked. The revised procedure includes the intervals for all devices as well as the basis. The procedure will be reviewed with the contractor that is selected to perform the test in the future. The contractor will also be given a copy of the procedure.	5/6/2011	5/16/2011	Admits
Texas RE	Bosque Power Company, LLC	NCR10247	TRE200900135	Settlement Agreement	Bosque failed to perform functional test of trip circuits. The work was supposed to be done by contractors and plant personnel did not notice the omission until November 2009. There are a total of 212 generation Protection System devices in the Bosque plant, 49, or 23% of the plant lockout relays and protective relays were non-compliant.	PRC-005-1	2	Lower	Lower	This violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system because functional trip testing of the plant protective systems was due in May 2008 and was actually completed in November 2009. 49 relays out of 212 total protection devices lacked functional testing. No issues were found when the trip circuits were function tested in November 2009.	5/1/2008	11/30/2009	$13,000 (for TRE200900134 and TRE200900135)	Self-Report	This violation was the result of an oversight failure by the contractor hired to perform relay test and protection system functional test. It was also an oversight failure by plant personnel for not confirming all of the required tests were performed. To prevent such oversight failures from occurring again, Bosque's procedure has been revised to include a specific task to ensure that none of the required tests are overlooked. The procedure will be reviewed with the contractor that is selected to perform the test in the future. The contractor will also be given a copy of the procedure.	5/6/2011	5/16/2011	Admits
Texas RE	Wise County Power Company, LLC	NCR04165	TRE201000270	Settlement Agreement	Wise County was unable to provide evidence that a generation Protection System maintenance and testing program existed and was in place from June 28, 2007 to November 12, 2007.	PRC-005-1	1	High	Severe	This violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system because a written Protection System maintenance and testing program was missing for five months but actual tests on most of the equipment were performed.	6/28/2007	11/13~~12~~/2007	$12,000 (for TRE201000270 and TRE201000271)	Self-Report	A written Protection System maintenance and testing procedure was put in place on November 13, 2007. All Protection System devices were tested between October 2009 and March 2010 with no issues found.	11/13/2007	7/15/2011	Admits
Texas RE	Wise County Power Company, LLC	NCR04165	TRE201000271	Settlement Agreement	Wise County had not performed maintenance and testing on some of its generation Protection System devices within the stated intervals required by its generation Protection System maintenance and testing program dated November 13, 2007. Of 150 Protection System devices, 16 (10.7%) were completed outside the documented test interval and 20 items (13.3%) had incomplete documentation on the previous tests. Wise County completed testing on its entire Protection System between October 2009 and March 2010 with no issues found with the devices.	PRC-005-1	2	Lower	Lower	This violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system because less than 25% of the total Protection System devices were tested outside the specified intervals. No issues were found and devices operated as expected until the issue was mitigated.	6/28/2007	3/1/2010	$12,000 (for TRE201000270 and TRE201000271)	Self-Report	A written Protection System maintenance and testing procedure was put in place on November 13, 2007. All Protection System devices were tested between October 2009 and March 2010 with no issues found.	3/1/2010	7/15/2011	Admits

Attachment A-1

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
Texas RE	Frontera Generation Limited Partnership	NCR04072	TRE201000170	Settlement Agreement	Frontera had inadvertently missed a request for information concerning its generator step-up transformer. The request for information had been sent from its associated Transmission Planner, on March 29, 2010. The requested data was provided to the Transmission Planner on June 9, 2010. As a result, Frontera did not provide generator transformer information to its associated Transmission Planner, AEP Transmission (AEP), within 30 calendar days of the request, as required by the Standard.	VAR-002-1.1a	4	Lower	Lower	This violation posed a minimal and did not pose a serious or substantial risk to the reliability of the bulk power system and had a minimal impact because the violation is related to a late submission of requested data that is used for system models and development of generator bus voltage and reactive power models. Also, the data finally provided to the AEP Transmission Planner was identical to data provided in previous years.	4/29/2010	6/9/2010	$5,000	Self-Certification	Frontera supplied data to the Transmission Planner when the situation was discovered, and promptly mitigated the immediate violation. To prevent recurrence, Frontera completed mandatory re-training on the requirements of NERC standard VAR-002-1.1a to improve awareness of facility management. Frontera also developed and sent a letter to the associated Transmission Planner requesting that it change the process for future information requests to ensure a similar communication breakdown will not occur. This will include communication to multiple site personnel, appropriate priority indication on the email and a hard copy delivered via registered mail. A letter from the Head of Upstream Power organization, which manages the power plant facilities in Texas, was sent to the subject employee reinforcing the importance of complying with all NERC Reliability Standards and appropriately responding to formal requests from industry counter parties.	6/30/2011	8/3/2011	Neither Admits nor Denies
WECC	Northwestern Corporation (NWC)	NCR05282	WECC201102380	Settlement Agreement	On January 3, 2011, NWC self-reported a violation of WECC Regional Standard IRO-STD-006-0 WR1, stating that it failed to provide Unscheduled Flow (USF) relief for a USF event on WECC Qualified Transfer Path 66. The Path Operator initiated a USF procedure and NWC was required to provide relief to Path 66 by curtailing a restricted transmission. NWC created a transaction for 40 MW on the this Path after the USF event had been called and thus failed to provide a relief obligation of 2.4 MW and take alternate action to relieve the Path.	IRO-STD-006-0	WR1	Not applicable because the standard is regional	Not applicable because the standard is regional	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NWC's increased flow on the Path was virtually undetectable. The Path operator was capable of curtailing transactions on the Path to reduce loading in the event of a overload but the operator did not have to resort to curtailment.	6/17/2010	6/17/2010	$0	Self-Report	NWC performed training for all System Operators that perform the scheduling/Balancing Authority function. These are the Operators who would be performing the USF relief. Included in this submission is email correspondence indicating that all the applicable System Operators have been trained on the necessity to manually refresh this screen prior to reviewing/approving Requests for Interchange.	1/3/2011	2/24/2011	Does Not Contest
WECC	Northern Lights/PNGC (NLI)	NCR05279	WECC201002326	Settlement Agreement	NLI self-reported noncompliance with PRC-008-0 R1 and R2 on December 6, 2010. Based on the Self-Report, WECC determined that NLI did not have an Under Frequency Load Shedding (UFLS) maintenance and testing program.	PRC-008-0	R1	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because during a potential UFLS event, NLI would shed no more than 11.95 MW of load in the summer and 17.22 MW in the winter, which is a small amount relative to the load that would be shed in the Northwest during an UFLS event. The equipment was properly functioning and maintained despite the lack of a formal maintenance program.	6/18/2007	5/27/2011	$0	Self-Report	NLI created a list of their UFLS equipment and a formal Maintenance and Testing Program. NLI determined which equipment needs to have maintenance and testing preformed and then performed the required maintenance and testing.	3/4/2011	8/26/2011	Does Not Contest
WECC	Northern Lights/PNGC (NLI)	NCR05279	WECC201002327	Settlement Agreement	NLI self-reported noncompliance with PRC-008-0 R1 and R2 on December 6, 2010. WECC determined that NLI failed to provide evidence to demonstrate implementation of an Under Frequency Load Shedding (UFLS) maintenance and testing program.	PRC-008-0	R2	Medium	Severe	This violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because during a potential UFLS event, NLI would shed no more than 11.95 MW of load in the summer and 17.22 MW in the winter, which is a small amount relative to the load that would be shed in the Northwest during an UFLS event. The equipment was properly functioning and maintained despite the lack of a formal maintenance program.	6/18/2007	5/27/2011	$0	Self-Report	NLI created a list of their UFLS equipment and a formal Maintenance and Testing Program. NLI determined which equipment needs to have maintenance and testing preformed and then performed the required maintenance and testing.	3/4/2011	8/26/2011	Does Not Contest

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900245	Settlement Agreement	Nineteen employees who no longer needed access to Critical Cyber Assets (CCAs) due to internal job transfer were not removed from FRCC_URE1's access list within 7 days, as required by the Standard.	CIP-004-1	R4	Lower	Lower	This violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the nineteen employees in question were long-term company employees who originally had access but were later assessed to no longer require direct access to CCAs. The employees had prior access with the proper PRAs and training, which met all prerequisites for CCA access.	10/30/2008* *On 10/22/2008, personnel were transferred and access was required to be removed no later than 10/29/2008.	4/15/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Entity evaluated whether its personnel who had access to CCA had a continued need to such access - 9/4/2009 2. The list of all personnel with CCA access was corrected and the entity continued to monitor the list - 10/1/2009 3. Investigated the extent of the violation and determined how many people continued to have access after seven calendar days - 10/1/2009 4. Trained all supervisors - 10/15/2009 5. Entity considered how to strengthen manual controls for CIP-004 - 10/30/2009 6. With FRCC_URE1 Information Management as a lead, conducted review of control processes - 10/30/2009 7. Implemented recommendation for process improvement - 1/13/2010 8. Tested the effectiveness of revised processes - 3/20/2010 9. Analyzed the test results of Milestone 3 - 4/9/2010 10. Taskforce implemented additional improvements based on results of Milestone 4 - 4/15/2010 11. R2 and R3 Revised all necessary processes procedures and record management system - 1/19/2010 12. R2 and R3 - Provided any available data or evidence to compliance organization to demonstrate compliance - 1/19/2010 13. R2 and R3 - Included R2 and R3 compliance as a part of the Taskforce and determined if process could be improved to make it consistent with the remaining milestones for R4 - 4/15/2010	4/15/2010	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900265	Settlement Agreement	The entity's firewall at its emergency backup system (EBS) was configured to allow "any-any" default rules even after the system was put into production and was not configured to deny all rule and all explicit access privileges, in violation of this Standard.	CIP-005-1	R2.1	Medium	Lower	This violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the entity's firewall, which was not configured for deny all rule and all explicit access privileges had only allowed communication from a controlled environment and a trusted network, the primary control center Electronic Security Perimeter (ESP) for the primary control center.	7/1/2009	9/17/2009 (on 9/17/2009 the deny "any-any" rule was replaced)	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Replaced "any-any" rule with a default deny for ESP at entity's EBS - Completed before submission date 9/28/2009 on 9/17/2009 2. Determined if "any-any" rule existed in any other access point -9/28/2009 3. Reviewed and revised the entity's process for change management controls for ESP - 10/5/2009 4. Began deployment of training - 10/5/2009 5. Completed training to reinforce entity's controls - 10/19/2009	11/2/2009	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900298	Settlement Agreement	Twenty-four (24) employees with access to Critical Cyber Assets (CCAs) were not trained within 90 days from the date of granting access to the CCAs.	CIP-004-1	R2.1	Medium (NERC database states R2 Lower)	Lower	This violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the employees were long-term company employees who were added to the CCA access list and had a previous understanding of the company's cyber security controls.	7/1/2008	4/15/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Entity evaluated whether its personnel who had access to the CCA had continued need for such access - 9/4/2009 2. The entity's list containing all personnel with access to the CCA was corrected and the entity continues to monitor the list - 10/1/2009 3. The entity investigated the extent of the violation and determined how many personnel did not have their access revoked within seven calendar days - 10/1/2009 4. Trained all of its supervisors - 10/15/2009 5. Entity considered how to strengthen manual controls for CIP-004 - 10/30/2009 6. With FRCC_URE1 Information Management as lead, conducted a review of its control processes - 10/30/2009 7. Implemented recommendations for process improvement - 1/13/2010 8. Tested the effectiveness of its revised processes - 3/20/2010 9. Analyzed the test results of Milestone 3 - 4/9/2010 10. Taskforce implemented additional improvements based on results of Milestone 4 - 4/15/2010 11. R2 and R3 Revised all necessary processes procedures and record management system - 1/19/2010 12. R2 and R3 - Provided any available data or evidence to compliance organization to demonstrate compliance - 1/19/2010 13. R2 and R3 - Included R2 and R3 compliance as a part of the Taskforce and determined if process can be improved consistent with remaining milestones for R4 - 4/15/2010	4/15/2010	8/25/2010	Neither Admits nor Denies

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900299	Settlement Agreement	The entity was not able to retrieve records out of its records management system for six personnel to prove that personnel risk assessments were performed for these six employees.	CIP-004-1	R3	Medium	Moderate	This violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the employees were long-term company employees who were added to the Critical Cyber Asset (CCA) access list and had a previous understanding of the company's cyber security controls.	7/1/2008	1/19/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Entity evaluated whether entity personnel with access to the CCA had a continued need for such access - 9/4/2009 2. FRCC_URE1's list with all personnel with CCA access was corrected and FRCC_URE1 continues to monitor the list - 10/1/2009 3. Investigated the extent of the violation and determined how many people continued to have access after seven calendar days - 10/1/2009 4. Trained its supervisors - 10/15/2009 5. Considered how to strengthen its manual controls for CIP-004 - 10/30/2009 6. With FRCC_URE1 Information Management as lead, conducted review of control processes - 10/30/2009 7. Implemented recommendations for process improvement - 1/13/2010 8. Tested the effectiveness of its revised processes - 3/20/2010 9. Analyzed the test results of Milestone 3 - 4/9/2010 10. Taskforce implemented additional improvement based on the results of Milestone 4 - 4/15/2010 11. R2 and R3 Revised all necessary processes procedures and record management system - 1/19/2010 12. R2 and R3 - Provided any available data or evidence to compliance organization to demonstrate compliance - 1/19/2010 13. R2 and R3 - Included R2 and R3 compliance as a part of the Taskforce and determined if process can be improved consistent with remaining milestones for R4 - 4/15/2010	4/15/2010	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900300	Settlement Agreement	The entity had a system with multiple applications that allowed access to both non-cyber and Cyber Assets. Employees without personnel risk assessments (PRAs) were able to access non-cyber asset applications on the system. It was determined that the system should have been designated as a physical access control system and therefore all employees with access should have had valid PRAs.	CIP-006-1	R1.8	Lower	Lower	This violation did not pose a serious or substantial risk to the bulk power system (BPS) because the entity's system used for physical access control was in a controlled Physical Security Perimeter (PSP) and although the entity's personnel (with no PRAs) were allowed to access the system applications, they did not have any privileges to control physical access of the entity's Critical Cyber Asset (CCA) infrastructure.	7/1/2009	1/7/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Assembled list of entity employees with access to concerned access control and monitored system and processed PRAs - 12/5/2009 2. Checked to see if any other similar assets were not protected and entity implemented a plan within 3 days - 12/10/2009 3. Updated cyber security policy to clarify that all such Cyber Assets and CCAs must be protected - 12/30/2009 4. Instructed or trained all entity employees and contractors as applicable on the updated policy and procedure - 1/7/2010 5. Completed all outstanding PRAs for employees and contractors with access to Picture Perfect and maintained list of employees and revoked access for those who failed, and documented revocation - 1/7/2010	1/7/2010	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900301	Settlement Agreement	The entity was to create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system and its operation. - The entity self-reported that its test procedure did not address adverse effects to the production environment and were focused solely on application and functionality testing instead of also including specific instructions for testing cyber security controls.	CIP-007-1	R1.1	Medium	Lower	This violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS) because the entity was performing testing in a proper environment although it was only testing for functionality. Additionally all system changes were sourced from trusted and vendor approved sources. The functional testing addressed some security vulnerabilities.	7/1/2008	1/29/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Modified entity's testing procedure to include cyber security controls for all significant changes - 12/15/2009 2. Developed training class for entity personnel related to the change management process - 12/15/2009 3. Performed complete review of all Cyber Assets within the Electronic Security Perimeter (ESP) and compiled a list of non-compliant assets as per CIP-007 R1 - 12/15/2009 4. Developed a plan to bring non-compliant assets back in compliance - 12/15/2009 5. Started implementation of the ports and services plan - 12/21/2009 6. Started delivery of CIP-007 training - 12/21/2009 7. Completed training of CIP-007 for all applicable personnel responsible for change - 1/14/2010 8. Completed all tasks related to the ports and services plan - 1/29/2010	1/29/2010	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900302	Settlement Agreement	The entity did not include 115 system operator workstations as part of its ports and services review.	CIP-007-1	R2.1	Medium	Lower	This violation did not pose a serious or substantial risk to the bulk power system (BPS) because the operator's workstations were based on vendor approved configurations and system applications.	7/1/2009	1/29/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Modified entity's testing procedure to include cyber security controls for all significant changes - 12/15/2009 2. Developed training class for entity personnel related to the change management process - 12/15/2009 3. Performed a complete review of all Cyber Assets within the Electronic Security Perimeter (ESP) and compiled a list of non-compliant assets as per CIP-007 R1 - 12/15/2009 4. Developed a plan to bring non-compliant assets back in compliance - 12/15/2009 5. Started implementation of the ports and services plan - 12/21/2009 6. Started delivery of CIP-007 training - 12/21/2009 7. Completed training of CIP-007 for all applicable personnel responsible for change - 1/14/2010 8. Completed all tasks related to the ports and services plan - 1/29/2010	1/29/2010	8/25/2010	Neither Admits nor Denies

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000350	Settlement Agreement	The entity did not identify twelve (12) Cyber Assets as Critical Cyber Assets (CCAs).	CIP-002-1	R3	High	Lower	This violation did not pose a serious or substantial risk to the bulk power system (BPS) because all of the assets were protected by standard company security control practices for logical and physical access and the portable Cyber Assets were in protective custody of the control center.	7/1/2008	6/1/2011	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Spot Check	The entity added the newly identified Critical Cyber Assets (CCAs) to the official lists, developed a checklist of all policies, procedures and other documentation and further implemented all of the required controls for the newly identified CCAs to comply with CIP-002 through CIP-009.	6/1/2011	8/10/2011	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000351	Settlement Agreement	The entity did not make the cyber security policy readily available to 12 of its remote contractors who had only logical access to its Critical Cyber Assets (CCAs) until March 25, 2010.	CIP-003-1	R1.2	Lower	Lower	This violation did not pose serious or substantial risk to the bulk power system (BPS) because the contractors remotely accessed the system and were from reputable companies that supported entities cyber systems and were well aware of the applicable cyber security controls.	7/1/2008	3/24/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Spot Check	1. Contractors (who had access to or were responsible for CCAs) were provided a copy of the entity's cyber security policy.	3/25/2010	8/25/2010	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000391	Settlement Agreement	In two instances, the entity did not include the effect of ramp rates which were identical and agreed to between affected BAs in the Scheduled Interchange values to calculate Area Control Error (ACE). There were two FRCC_URE1 Interchange Transaction Tags (tags) that did not identify the ramp rate start/stop times (Null value). As evidenced in the tags, the default used by FRCC_URE1 and the other party to the tag for these null tags were not the same ramp rate and did not accurately include the effect of ramp rate in its schedule Interchange value to calculate ACE.	BAL-005-0.1b	R11	Medium	Severe	This violation did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. The mismatch was limited to a 10 or 20 minute ramp rate of 35 MW in the Scheduled Interchange between affected BAs and there were no subsequent violations reported for Control Performance Standards (CPS1 and CPS2) for BAL-001-0a by the affected entities. 2. The only potential effect to the BPS has been a temporary increase in inadvertent energy during the ramp times. 3. The impact is also minimized due to the small number of the tags (2) which had this mismatch in ramp times and the ramp was only between a rate of ten minutes (10) at one BA and twenty (20) minutes at the other BA.	6/22/2009 (first blank tag)	11/13/2009 (rejection of blank tags)	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Spot Check	1. Instituted procedures and instructed FRCC_URE1 coordinators to reject any electronic tag (E-tag), except E-tags for cancellation, termination, curtailment and reload unless there are actual values in the ramp duration fields and the fields match; 2. Automated software enhancements in FRCC_URE1 computer systems to ensure that an E-tag is not accepted unless there ~~is~~ are matching ramp durations in both fields unless the operator re-confirms and verifies that it is correct. FRCC_URE1's procedures on E-tags were also modified to include the automatic software enhancements; and 3. FRCC_URE1 coordinators received follow-up training with attention to those steps implemented to strengthen FRCC_URE1's compliance with the BAL-005-0.1b.	1. 11/13/2009 2. 11/30/2009 3. 12/31/2009	8/11/2011	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000393	Settlement Agreement	The entity did not make its cyber security policy readily available to nineteen of its contractors, who had authorized access to its Critical Cyber Assets (CCAs).	CIP-003-1	R1.2	Lower	Lower	This violation did not pose serious or substantial risk to the bulk power system (BPS) because the contractors remotely accessed the system and were from reputable companies that supported entity's Cyber Assets and were well aware of applicable cyber security controls.	12/31/2009	8/27/2010	$38,000 (for FRCC200900245, FRCC200900265, FRCC200900298, FRCC200900299, FRCC200900300,FRCC200900301, FRCC200900302, FRCC201000350, FRCC201000351, FRCC201000391, and FRCC201000393)	Self-Report	1. Placed a copy of the cyber security policy at a central location and explained on the Physical Security Perimeter (PSP) sign in,sign out log the availability of the cyber security policy. 2. E-mailed a copy of the cyber security policy to each contractor with remote authorized cyber access.	8/27/2010	5/4/2011	Neither Admits Nor Denies
NPCC	NPCC_URE1	NCRXXXXX	NPCC201100245	Notice of Confirmed Violation	In December 2010, three retired NPCC_URE1 employees were contracted to perform the function of safety observer. These three contractors were provided with access credentials that allowed them to enter the physical security perimeters (PSPs) for critical cyber assets. These credentials consisted of a special key and electronic token. On January 28, 2011 Corporate Security began investigating a report that the contractors left NPCC_URE1 property without returning the access credentials. Corporate Security simultaneously disabled the electronic access cards issued to the contractors. On February 1, 2011 the incident was reported to and reviewed to by the NERC Compliance group. In summary: The termination date was 12/30/2010. The electronic badges were deactivated on 1/28/2011. The keys were returned on the following dates: 1/4/11, 1/28/2011, 2/2/2011	CIP-004-3	4.2	Medium	Moderate	NPCC determined that the violation posed a minimal and did not pose a serious or substantial risk to the bulk power system because NPCC_URE1 showed that the contractors were former NPCC_URE1 employees and made no unauthorized ESP/PSP access attempts. In addition the three contractors completed the cyber security training and had a Personnel Risk Assessment completed at the time of hire.	12/31/2010	3/3/2011	$3,500	Self-Report	Upon notification of the incident NPCC_URE1 deactivated badges and collected keys. The responsible manager was explained what the the NERC requirements and NPCC_URE1 process are, while this incident was investigated by the NERC Compliance Group. Corporate security issued a paper letter and email to all Managers and Supervisors in NPCC_URE1. MItigating measures include the issuance of an awareness message to the person receiving credentials that allow unescorted access to a physical security perimeter. The message will notify the person to immediately report a lost/stolen credential and to return credentials prior to last day.	3/3/2011	7/26/2011	Does not Contest, Accept

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
NPCC	NPCC_URE2	NCRXXXXX	NPCC201000169	Notice of Confirmed Violation	NPCC_URE2 did not have a complete set of documentation showing that the four (4) Access Control Systems (ACS) that control the physical access to URE's Physical Security Perimeters were afforded all the protective measures specified in the standards and requirements listed under CIP-006-1 R1.6 as of 12/31/09.	CIP-006-1	1.6	Medium	Lower	NPCC determined that the violation posed a minimal and did not pose serious or substential risk to the reliability of the bulk power system (BPS) because even though the ACSs may have not been fully afforded all the protective measures as required by CIP-006-1 R 1.6, NPCC_URE2 has historically and consistently restricted electronic and physical access to these systems and has allowed access strictly to individuals who have a functional need. Also, there have been no known issues or evidence of misuse or unauthorized access to these cyber assets.	1/1/2010	4/30/2011	$6,000 (for NPCC201000169, NPCC201000170, NPCC201000171, NPCC201000172)	Self- Report	1. NPCC_URE2 engaged a Consultant to conduct a compliance audit of the four (4) Access Control Systems (ACS). The project objectives were to assess and confirm each ACS for applicable compliance requirements, document the evidence of current conditions, and develop a Gap Analysis for remaining compliance work. 2. NPCC_URE2 conducted training of all Human Capital responsible for the Access Control Systems to ensure that all personnel are aware of their responsibilities associated with the Access Control Systems. 3. NPCC_URE2 developed and implemented a work plan to address all audit findings.	4/30/2011	6/9/2011	Does not Contest
NPCC	NPCC_URE2	NCRXXXXX	NPCC201000170	Notice of Confirmed Violation	A review of the Critical Infrastructure Management System (CIMS) Security Patch Notification report discovered that the assigned patch coordinator for these assets did not document the assessment of six (6) security patches or upgrades for applicability within thirty (30) calendar days of their availability as required by CIP-007-2a R3.1.	CIP-007-2a	3.1	Lower	N/A	NPCC determined that the violation posed a minimal and did not pose a serious or substential risk to the reliability of the bulk power system (BPS) because as provided for in NPCC_URE2's Patch Management program, the third-party patch monitoring service vendor notified URE of the patch releases and URE's assigned subject matter expert (SME) acknowledged the applicability of the patches as required, but the acknowledgement exceeded the thirty (30) day window by five (5) days for five of the patches and six (6) days for one of the patches. The delayed acknowledgement did not affect the determination of the patches' applicability. The delay impacted the execution of the process that generates the documentation of applicability.	5/14/2010	5/19/2010	$6,000 (for NPCC201000169, NPCC201000170, NPCC201000171, NPCC201000172)	Self- Report	1. The applicable patch notifications were fully processed in NPCC_URE2's Critical Infrastructure Management System (CIMS), which documented the assessment of the security patches for applicability. 2. An additional staff member was assigned to perform the role of a secondary 30-day Patch Subject Matter Expert (SME) and to review patch alerts as they are received from a third-party source. In cooperation with the primary SME, this staff member documents the assessment of the security patches for applicability in CIMS within thirty days of availability. 3. Monthly meetings of the NPCC_URE2 Cyber Security Management Team (CSMT) are held to ensure that the security patch management requirements are being met as expected. 4. Training was conducted on the patch management process with all applicable Human Capital.	12/29/2010	3/29/2011	Does not Contest
NPCC	NPCC_URE2	NCRXXXXX	NPCC201000171	Notice of Confirmed Violation	NPCC_URE2 did not implement compensatory measures such as procedural controls following the suspension of the technical controls (electronic login/logout process) on three Critical Cyber Assets for a period of 5 calendar days between 04/22/2010 and 04/26/2010.	CIP-007-2a	5	Lower	N/A	NPCC determined that the violation posed a minimal and did not pose a serious or substential risk to the reliability of the bulk power system (BPS) because, even though the technical controls were suspended during this period, the cyber asset remained secured within the facility's control room physical security perimeter and was staffed on a continuous 24 hour basis by authorized users.	4/22/2010	4/26/2010	$6,000 (for NPCC201000169, NPCC201000170, NPCC201000171, NPCC201000172)	Self-Report	1. A procedure was developed to ensure that the necessary compensatory measures are in place following the suspension of the technical controls. 2. Training was conducted on the new procedure with all applicable Human Capital.	11/19/2010	3/31/2011	Does not Contest
NPCC	NPCC_URE2	NCRXXXXX	NPCC201000172	Notice of Confirmed Violation	NPCC_URE2 reclassified five (5) Generator Control System (GCS) consoles in the Turbine Gallery as non-Critical Cyber Assets (CCAs) and reconfigured the Electronic Security Perimeter (ESP) to exclude the GSC consoles, in effect redeploying former CCAs outside the ESPs without erasing the data storage media.	CIP-007-2a	7.2	Lower	N/A	NPCC determined that the violation posed a minimal and did not pose a serious or substential risk to the reliability of the bulk power system (BPS) because, even though the Turbine Gallery GCS consoles were redeployed outside the defined ESP, they were never relocated outside the identified Physical Security Perimeter and electronic access controls remain active (individual user accounts were changed to read only). The Turbine Gallery GCS consoles are located in the Turbine Gallery which is a non-public area, located behind multiple security levels.	4/8/2010	9/24/2010	$6,000 (for NPCC201000169, NPCC201000170, NPCC201000171, NPCC201000172)	Self-Report	1. The applicable cyber assets' data storage media was erased or destroyed. 2. An internal review board to oversee change management, including Cyber Asset disposal and redeployment was established. 3. Review of processes for Cyber Asset disposal & redeployment performed and identified changes necessary to ensure compliance with CIP-007-2a R7.2 was implemented. 4.Training was conducted to reinforce the change control process (including Cyber Asset disposal and redeployment) with all applicable Human Capital.	11/18/2010	3/31/2011	Does not Contest

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	SERC_URE1	NCRXXXXX	SERC201000726	Notice of Confirmed Violation	SERC_URE1, as a Load Serving Entity, violated CIP-003-1 R2 for failure to assign a senior manager with overall responsibility for leading and managing SERC_URE1's implementation of, and adherence to, standards CIP-002 through CIP-009. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-003-1	R2	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4; 2. SERC_URE1 had a senior manager tasked with the responsibility of approving the risk based methodology, the list of critical assets, and the list of critical cyber assets for the CIP-002 self-certifications; however, SERC_URE1 had not formally designated and documented the senior manager with the specificity required by the Standard.	12/31/2008	12/10/2010	$0	Self-Report	SERC_URE1 designated the Director of Electric Utilities as the senior manager with the responsibility for leading and for managing SERC_URE1's adherence to Standards CIP-002 through CIP-009.	12/10/2010	2/25/2011	Admits
SERC	SERC_URE1	NCRXXXXX	SERC201100765	Notice of Confirmed Violation	SERC_URE1, as a Load Serving Entity, violated CIP-002-1 R1 because its risk-based assessment methodology (RBAM) did not specifically address each of the asset types as required by the Standard. The violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-002-1	R1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4; and 2. SERC_URE1 does not own or operate any elements of the BPS and is a minimal size distribution utility with a load of less than XXX MW.	12/31/2009	6/1/2011	$0	Self-Report	SERC_URE1 revised its RBAM to address each asset types including its procedures and evaluation criteria as required by the Standard.	6/1/2011	6/10/2011	Admits
SPP RE	SPP RE_URE1	NCRXXXXX	SPP200900136	Settlement Agreement	On October 5, 2009, SPP RE_URE1 submitted a Self-Report for violation of CIP-006-1 R1. The violation occurred on September 9, 2009, when an SPP RE_URE1 employee (backup transmission control center operator) granted unescorted access to two individuals, an SPP RE_URE1 security guard and contractor (HVAC technician), into SPP RE_URE1's backup transmission control center (BUTCC), which is inside SPP RE_URE1's physical security perimeter. Neither the SPP RE_URE1 security guard nor the contractor had authorized unescorted access to the BUTCC. Consequetly, SPP RE_URE1 violated CIP-006-1 R1 by failing to maintain the implementation of its *CIP Physical Security Compliance Policy* . Specifically, on September 9, 2009, a HVAC technician went to SPP RE_URE1's facility to complete some repairs in SPP RE_URE1's BUTCC. A security guard escorted the HVAC technician to the 4th floor of SPP RE_URE1's facility, which is where the BUTCC is located. After entering the lobby of the 4th floor, the HVAC technician told SPP RE_URE1's Transmission Training Coordinator that he needed access to the BUTCC to complete some maintenance work. As required by SPP RE_URE1's policy, the Transmission Training Coordinator required the security guard and HVAC technician to complete the sign-in logbook. The Transmission Training Coordinator then stated that all transmission personnel were in a staff meeting, and therefore, unable to escort them into the BUTCC. While waiting for an authorized escort, a transmission employee who was working near the back door of the BUTCC used his ID badge to open the door and allow the security guard and HVAC technician access to the BUTCC. According to SPP RE_URE1's investigative report, the transmission employee recognized the HVAC technician because he had recently been making repairs to the HVAC system in the BUTCC. Furthermore, the investigative report noted that the transmission employee believed that the security guard had authorized access to the BUTCC. Because the transmission employee propped the door open, a door alarm was triggered, which in turn, caused an alarm in the Security Operations Center (SOC). The door was propped open for 51 seconds, allowing the HVAC technician to install wires that were outside the BUTCC through the BUTCC. The SOC employee followed SPP RE_URE1's procedure by calling the on-duty security supervisor to dispatch security to investigate the door alarm. The security supervisor immediately contacted the security guard that escorted the HVAC technician to the 4th floor. The security guard explained to his supervisor that he was the only one escorting the HVAC technician in the CIP area. The security supervisor instructed the security guard and HVAC technician to immediately vacate the BUTCC because the security guard was not authorized to be	CIP-006-1	R1.6	Medium	Severe	This violaiton did not pose serious or substantial risk to the reliability of the bulk power system (BPS). Although the HVAC technician was not escorted by an employee authorized for such unescorted physical access into the BUTCC, the technician had been requested by SPP RE_URE1 to perform required maintenance on its HVAC system, which consisted of CIP and non-CIP areas. The technician was accompanied the entire time by an SPP RE_URE1 security guard who, with his presence alone, provided assurance that no damage or compromise to SPP RE_URE1's CIP assets could occur. Both the security guard and the HVAC technician completed the sign-in logbook. Additionally, although the security guard was not escorted by an employee authorized for unescorted physical access, he had completed training and had a clear background check, as required by CIP-004-1 R2 and R3.	9/9/2009	9/9/2009	$6,000	Self-Report	SPP RE_URE1 took immediate steps to correct the violation and prevent any further occurrence by: 1. conducting a prompt investigation of the violation; 2. documenting the results of the investigation in an *SPP RE_URE1 Security Services Investigation Report;* 3. advising the SPP RE_URE1 CEO and all SPP RE_URE1 managers of the violation; and 4. carrying out corrective actions to prevent further occurrences, which included: a. providing a memorandum from the CEO with attached SPP RE_URE1's *CIP Physical Security Compliance Policy* (Policy) to all SPP RE_URE1 employees and contractors notifying them of the violation and SPP RE_URE1's expectation of compliance with the Policy; b. counseling the individuals who violated the Policy, ensuring their understanding of the Policy going forward; and c. management review of the Policy with all SPP RE_URE1 employees and contractors.	12/7/2009	1/11/2010	Neither Admits nor Denies
SPP RE /RF	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900152 RFC200900323	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities concluded that the 2008 version of SPP RE_URE1/RFC_URE1's cyber security policy explicitly referenced a company standard that did not conform to the CIP Standards. Specifically, although CIP-007-1 R5.3.2 requires each password to consist of a combination of three elements (alpha, numeric, and special characters), SPP RE_URE1/RFC_URE1's cyber security policy required only two password elements. Additionally, SPP RE_URE1/RFC_URE1 failed to reference its separate company CIP-002 through CIP-009 policies and procedures in its 2009 version of its cyber security policy. Therefore, there was no linkage from the cyber security policy to the company standards and procedures to demonstrate that the cyber security policy addressed all the requirements of CIP-002 through CIP-009, as required by CIP-003-1 R1.1.	CIP-003-1	R1.1	Lower	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS) because SPP RE_URE1/RFC_URE1's password protection for system access required two elements: SPP RE_URE1/RFC_URE1 had robust policies in place to secure its cyber security assets, and there was no evidence of any unauthorized system access. Additionally, SPP RE_URE1/RFC_URE1 had company policies and procedures in place addressing CIP-002 through CIP-009 but SPP RE_URE1/RFC_URE1 simply failed to reference such policies and procedures in its cyber security policy.	7/1/2008	12/31/2009	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 revised its cyber security policy to require passwords to consist of a combination of three elements as required by CIP-007-1 R5.3.2, and to reference applicable company standards to show compliance with Standards CIP-002 through CIP-009.	12/31/2009	3/25/2010	Neither Admits nor Denies

Greenwood Commissioners of Public Works

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SPP RE /RF	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900153 RFC200900324	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities concluded that SPP RE_URE1/RFC_URE1 violated CIP-003-1 R2 when it assigned three SPP RE_URE1/RFC_URE1 managers with shared "senior manager" responsibilities for leading and managing SPP RE_URE1/RFC_URE1's implementation of, and adherence to, Standards CIP-002 through CIP-009.	CIP-003-1	R2	Medium	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS) because the managers with shared "senior manager" responsibilities for CIP compliance were assigned to the operating areas and functions for which they were closely related and had the responsibility of overseeing CIP compliance. Consequently, there was strict oversight of CIP compliance.	7/1/2008	12/21/2009	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 revised its senior manager designation to have a single senior manager identified with overall responsibilities for leading and managing the implementation of, and adherence to, Standards CIP-002 through CIP-009.	12/21/2009	3/29/2010	Neither Admits nor Denies
SPP RE /RF	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900154 RFC200900325	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities concluded that SPP RE_URE1/RFC_URE1's 2009 cyber security training program did not include instructional information pertaining to the proper use of Critical Cyber Assets (CCAs) as required by CIP-004-1 R2.2.1. Although SPP RE_URE1/RFC_URE1 included general references in its training materials and noted that affected employees must be authorized to gain access to CCAs, and that individuals must comply with CIP Standards, SPP RE_URE1/RFC_URE1's training materials had no references or instruction regarding the proper use of CCAs (e.g., personal use of CCAs, access to corporate business applications, access to the Internet, installation of unapproved software, and use of Cyber Assets by personnel not specifically authorized for electronic access in accordance with the CIP Standards). Consequently, the Regional Entities determined that such general references did not provide sufficient training for authorized personnel to understand the proper use of CCAs and to ensure compliance with the CIP Standards.	CIP-004-1	R2.2	Medium	Moderate	This violation posed a minimal risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1/RFC_URE1's cyber security training program did not include instructional information pertaining to the proper use of CCAs, SPP RE_URE1/RFC_URE1's cyber security training program did include instructional information pertaining to physical and electronic access controls to CCAs, proper handling of CCA information, and action plans and procedures to recover and access CCAs following a Cyber Security Incident, as required by CIP-004-1 R2.2.2 - R2.2.4.	7/1/2008	12/29/2009	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 revised its cyber security training program to include language explaining the purpose and proper use of CCAs.	6/28/2010	7/14/2010	Neither Admits nor Denies
SPP RE /RF	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900155 RFC200900326	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities discovered that while SPP RE_URE1/RFC_URE1 maintained lists of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) and their specific access rights, SPP RE_URE1/RFC_URE1's quarterly review did not include a review of the specific access rights of personnel.	CIP-004-1	R4.1	Lower	Moderate	This violation posed a minimal risk to the reliability of the bulk power system (BPS). SPP RE_URE1/RFC_URE1 did maintain an access list with specific access rights. Although SPP RE_URE1/RFC_URE1 did not review the specific access rights on a quarterly basis, it did review and modify (if necessary) access rights each time the status of an individual on the access list changed. Also, SPP RE_URE1/RFC_URE1 conducted quarterly reviews of its access list, which included reverification of each individual's status, verification of completion of the required annual cyber security training, and determination of the status of each individual's personnel risk assessment. Moreover, no personnel access rights were affected during or after the completion of the Mitigation Plan, and there was no evidence that any individual gained improper access to any of SPP RE_URE1/RFC_URE1's CCAs.	7/21/2008	9/9/2009	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 revised its access control procedures to include a quarterly review of each individual's specific access rights for both physical and electronic access.	6/28/2010	7/14/2010	Neither Admits nor Denies
SPP RE /RF	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900157 RFC200900328	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities discovered that SPP RE_URE1/RFC_URE1's Cyber Security Incident response plan (Incident Response Plan) did not include any documented procedures to characterize and classify events as reportable Cyber Security Incidents, as required by CIP-008-1 R1.1. Instead, SPP RE_URE1/RFC_URE1's Incident Response Plan required the applicable incident manager to consult with appropriate senior managers to determine if an incident was reportable. Additionally, SPP RE_URE1/RFC_URE1's Incident Response Plan contained a documentation error. Specifically, although the Incident Response Plan indicated that any changes to the procedures of the Incident Response Plan, once approved by management, are applied within 90 calendar days of the approval as required by CIP-008-1 R1.4, another section of the Incident Response Plan indicated that such changes were to be incorporated into the plan annually.	CIP-008-1	R1 (R1.1, R1.4)	Lower	High	This violation posed a minimal risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1/RFC_URE1 failed to include documented procedures in its Incident Response Plan that would characterize and classify events as reportable Cyber Security Incidents, SPP RE_URE1/RFC_URE1 verbally discussed and assessed potential reportable events, and if an event was deemed reportable, SPP RE_URE1/RFC_URE1 had comprehensive, documented procedures for reporting the event. Also, the contradictory statement regarding updating the Incident Response Plan within 90 calendar days of any changes was a typographical error.	7/1/2008	4/28/2010	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 revised its Incident Response Plan by adding procedures to characterize and classify events as reportable Cyber Security Incidents (CIP-008-1 R1.1) and corrected the typographical error to clarify that SPP RE_URE1/RFC_URE1 will update its plan within ninety calendar days of any changes to the plan (CIP-008-1 R1.4).	4/30/2010	5/11/2010	Neither Admits nor Denies

Attachment A-2

August 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet

PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SPP RE / RFC	SPP RE_URE1/ RFC_URE1	NCRXXXXX	SPP200900158 RFC200900329	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst Spot Check, the Regional Entities discovered that although SPP RE_URE1/RFC_URE1's recovery plans for Critical Cyber Assets (Recovery Plans) specified required actions in response to events or conditions of varying duration and severity for short-term events, the Recovery Plans failed to include a recovery phase for impacted facilities or assets after a mid-term or long-term event, such as a disaster. Instead, SPP RE_URE1/RFC_URE1's Recovery Plans referenced SPP RE_URE1/RFC_URE1's Business Continuity Plan (BCP) for response and recovery actions for "disaster" and "catastrophic" events. Although the BCP provided response procedures for disaster or catastrophic events, the BCP failed to include procedures to recover the affected Critical Cyber Assets from such events.	CIP-009-1	R1.1	Medium	High	The violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS). SPP RE_URE1/RFC_URE1 maintains a "hot" disaster recovery site and redundant systems for the Transmission Operator function that would become the primary operation site should the current operational site become inoperable from a disaster or catastrophic event. Although SPP RE_URE1/RFC_URE1's Recovery Plans did not specifically address events of varying duration and severity for the recovery of Critical Cyber Assets, SPP RE_URE1/RFC_URE1 did have plans whereby the critical transmission SCADA network assets are configured in a redundant manner and utilize redundant communication paths, i.e., there is always a "hot" standby or spare system with multiple diverse communication links to be utilized in the event of failure of a primary system or link.	7/1/2008	6/21/2010	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 modified its Recovery Plans to include recovery of Critical Cyber Assets in response to mid-term and long-term events.	7/13/2010	9/13/2010	Neither Admits nor Denies
SPP RE / RFC	SPP RE_URE1/RFC_URE1	NCRXXXXX	SPP200900159 RFC200900330	Settlement Agreement	During an October 29, 2009 joint SPP RE / ReliabilityFirst spot check, the Regional Entities concluded that SPP RE_URE1/RFC_URE1 could not provide adequate documentation demonstrating that its recovery plans for its Critical Cyber Assets (Recovery Plans) was exercised at least annually. SPP RE_URE1/RFC_URE1 did provide operator logs documenting a fail over and recovery of a SCADA server to an alternate control center; however, such documentation does not demonstrate that the Recovery Plans were exercised.	CIP-009-1	R2	Lower	High	The violation did not pose serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1/RFC_URE1 did not have documentation demonstrating that its Recovery Plans for Critical Cyber Assets were actually tested, SPP RE_URE1/RFC_URE1 had developed EMS/SCADA disaster recovery plans and conducted demonstrations of actual recovery from failure events. Additionally, SPP RE_URE1/RFC_URE1 maintains a "hot" disaster recovery site that would become the primary operation site should the current operational site become inoperable from a disaster or catastrophic event.	7/1/2008	7/1/2010	$10,000 (for SPP200900152 / RFC200900323; SPP200900153 / RFC200900324; SPP200900154 / RFC200900325; SPP200900155 / RFC200900326; SPP200900157 / RFC200900328; SPP200900158 / RFC200900329; and SPP200900159 / RFC200900330)	Spot Check	SPP RE_URE1/RFC_URE1 scheduled, conducted, and documented a paper tabletop drill to exercise the documented Recovery Plans for recovery from an actual incident.	9/28/2010	11/3/2010	Neither Admits nor Denies

Document Accession #: 20110831-5237 Filed Date: 08/31/2011

Document Content(s)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Minnkota Power Cooperative, Inc. - pdf page 31

City of Palo Alto - pdf page 36

Southwest Transmission Cooperative, Inc. - pdf page 36

RC12-11

April 30, 2012

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Find Fix and Track Report[1] (FFT) in Attachment A regarding 36 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 64 possible violations[5] of 18 Reliability Standards that posed a minimal risk to the reliability of the bulk power system (BPS). In all cases, the possible violations contained in this FFT have been found and fixed, so they are now described as "remediated issues." A certification of completion of the mitigation activities has been submitted by the respective Registered Entities.

As discussed below, this FFT includes 64 remediated issues. These FFT remediated issues are being submitted for informational purposes only. The Commission has encouraged the use of streamlined

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

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

enforcement processes for occurrences that posed a minimal risk to the BPS.[6] Resolution of these minimal risk possible violations in this reporting format is appropriate disposition of these matters, and will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards.

Statement of Findings Underlying the FFT

The descriptions of the remediated issues and related risk assessments are set forth in Attachment A.

This filing contains the basis for approval by NERC Enforcement staff, under delegated authority from the NERC Board of Trustees Compliance Committee (NERC BOTCC), of the findings reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), each Reliability Standard at issue in this FFT is identified in Attachment A.

Text of the Reliability Standards at issue in the FFT may be found on NERC's website at http://www.nerc.com/page.php?cid=2|20. For each respective remediated issue, the Reliability Standard Requirement at issue is listed in Attachment A.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the possible violations identified in Attachment A have been mitigated. The respective Registered Entity has submitted a certification of completion of the mitigation activities to the Regional Entity. These mitigation activities are subject to verification by the Regional Entity via an audit, spot check, random sampling, a request for information, or otherwise. These activities are described in Attachment A for each respective possible violation.

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

Statement Describing the Resolution[8]

Basis for Determination

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

Notice of Completion of Enforcement Action

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

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

Request for Confidential Treatment of Certain Attachments

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

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

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

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

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

Attachments to be included as Part of this FFT Informational Filing

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

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

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

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

Notices and Communications

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326-1001 (404) 446-2560 David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 david.cook@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 rebecca.michael@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326-1001
(404) 446-2560

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

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

cc: Entities listed in Attachment B

NERC

Attachment a

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

NERC

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR APRIL 2012 FIND FIX AND TRACK REPORT (FFT) INFORMATIONAL FILING

FOR FRCC:

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

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

FOR MRO:

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

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

FOR NPCC:

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

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

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

FOR RFC:

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

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

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

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

FOR SERC:

R. Scott Henry*
President and CEO
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8202
(704) 357-7914 – facsimile
shenry@serc1.org

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

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

Andrea B. Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

FOR SPP RE:

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

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

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

FOR TEXAS RE:

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

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

FOR WECC:

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

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

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

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

NERC

Attachment c

Notice of Filing

ATTACHMENT C

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
April 30, 2012

Take notice that on April 30, 2012, the North American Electric Reliability Corporation (NERC) filed a FFT Informational Filing regarding thirty six (36) Registered Entities in eight (8) Regional Entity footprints.

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

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

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

Comment Date: [BLANK]

Kimberly D. Bose,
Secretary

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Midwest Reliability Organization (MRO)	MidAmerican Energy Company (MEC)	NCR00824	MRO2012009155	VAR-002-1.1b	R3; R3.1	On November 17, 2011, MEC, as a Generator Operator (GOP), self-reported an issue with VAR-002-1.1b R3 because it failed to notify its associated Transmission Operator (TOP) within 30 minutes of a status or capability change on the automatic voltage regulator (AVR) and the expected duration of the change in status or capability. Following restoration of a wind farm to service, the automatic voltage control feature was not restored to operation at the time the wind turbine generators were put in service on November 1, 2011. The AVR was on during November 1, 2011 through November 3, 2011; however, it was not enabled (controlling the voltage).	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). MEC is vertically integrated, with both the GOP and TOP functions. The entity's TOP scheduled the planned outage for maintenance and reconnected the wind farm to the grid. Therefore, although the GOP did not notify the TOP, the TOP manages the AVR and was able to ensure reliable operation. As the TOP reconnected the wind farm to the grid, the TOP noticed the wind farm was not maintaining the voltage schedule as it should be and determined AVR was not functioning properly (AVR was on but not enabled; not controlling the voltage). The TOP dispatched personnel and the AVR was restored. Additionally, the entity's wind farm is connected to the BPS by 161 kV lines and is rated at approximately 161 MVA.	The issue was mitigated on November 3, 2011, when MEC corrected the AVR issue. On November 3, 2011, MEC's system operators, in the transmission control center acting as the entity's TOP function, determined that the wind farm voltage control was not properly functioning. Personnel were then dispatched to the site and the AVR was restored.
Midwest Reliability Organization (MRO)	Wisconsin Public Service Corporation (WPS)	NCR00952	MRO201100372	VAR-002-1.1b	R1	On August 3, 2011, WPS, as a Generator Operator (GOP), self-reported an issue with VAR-002-1.1b R1 for failing to operate each generator connected to the interconnected transmission system in the automatic voltage control mode (automatic voltage regulator (AVR) in service and controlling voltage) and did not notify its Transmission Operator (TOP). The entity discovered that the unit was operating by design in a constant Mvar control mode of the AVR. On October 1, 2010, after a controls upgrade to the GOP's AVR, the GOP notified the TOP that the unit was now operating in voltage control mode. Due to an error in the new control scheme, it was actually still controlling in Mvar control mode. The GOP notified the TOP of this on August 3, 2011. The issue was discovered during an independent compliance review of control logic for a similar control replacement project at another combustion turbine site. Following review of the proposed control logic and changes, the engineer performed a review of the control logic on the unit and identified the method of operation to be noncompliant with the Standard. Additionally, WPS failed to notify its TOP of going into MVAR control mode during shutdown for three other units.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The first unit at issue, a 63 MW unit which is not a base-load unit, is connected to the BPS at the same interconnection point as three other larger separate units (not the three units in the scope of the issue) totaling 448 MVA, which were operated in voltage control mode. On occasions when the 63 MVA unit was online, it provided a much weaker source than the other base-load units. The impact of the 63 MVA unit's control mode on the bus voltage was minimal because the larger units were providing the voltage control at the interconnection bus. Furthermore, the additional three units that were found to be in Mvar control mode during their shutdown sequence were also of minimal risk to the BPS due to the very small window of time in which they were operating in a different control mode, but still had the AVR in-service. The units were shutting down and not being operationally controlled in the same manner as they would have been while operating. Additionally, the units only ran 130 hours during the period of time they were in Mvar control mode while the TOP believed it was in voltage control mode. This represented less than 2% of the time.	WPS performed the following actions to mitigate the remediated issue: (1) notified its TOP on August 3, 2011 that the unit was only able to control to an Mvar set point when the AVR was in service; (2) conducted an extent of conditions review of all BPS generators to ensure voltage was being controlled at all times during unit operation. The information reviewed included operational data, functional descriptions in operating manuals, control logic and consultation with original equipment manufacturers; (3) notified the TOP as other gas turbines were identified in having a similar Mvar control mode through some period of operation; (4) modified the control logic to support voltage control of the generator when the AVR is in service as the primary mode of operation; and (5) verified with its TOP the status and capabilities of the AVR controls for each unit interconnected with the TOP. On March 26, 2012, MRO verified that the WPS completed its mitigation activities on March 14, 2012.
Northeast Power Coordinating Council, Inc. (NPCC)	ISO-NE	NCR07124	NPCC2012009158	PER-003-0	R1; R1.1	On January 5, 2012, ISO-NE, as a Reliability Coordinator, self-reported that an operator was not NERC-certified during a six-hour proficiency watch on December 28, 2010 due to an administrative issue. The operator had completed the required 200 training hours for re-certification, but failed to formally renew the Reliability Coordinator re-certification.	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 employee had completed the required continuing education hours for the Reliability Coordinator certification, but incurred an administrative issue when re-applying for NERC Certification renewal.	NERC reinstated the shift supervisor's certificate on the same day ISO-NE brought the matter to NERC's attention. The ISO-NE Performance, Training and Integration Group (OPTI) implemented a process to generate a monthly report showing the current continuing education hours and certificate expiration dates for all control room staff. The report is sent to system operations management. The manager of OPTI cross-checks the list against the control room staff organization chart and provides confirmation by email to the control room operations director that the list is complete. The mitigation activity was verified complete by NPCC.
Reliability*First* Corporation (Reliability*First*)	Camp Grove Wind Farm, LLC (Camp Grove)	NCR00214	RFC2011001095	FAC-009-1	R1	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit and discovered that Camp Grove, as a Generator Owner, had an issue with FAC-009-1 R1. Camp Grover has a Facility Ratings Methodology in place which requires it to develop Facility Ratings for its transmission conductors. Camp Grove owns nine miles of 138 kV transmission conductors between its substation and the Commonwealth Edison Company switchyard. Reliability*First* determined that the entity had an issue with the Standard since it failed to develop Facility Ratings for its 138 kV transmission conductors.	Reliability*First* determined that this remediated issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The risk posed to the reliability of the BPS was mitigated by the following factors. Camp Grove designed the wind turbine to be its most limiting element. As a result, when Camp Grove revised its Facility Ratings to include transmission conductors, Camp Grove did not have to change the most limiting element. In addition, Camp Grove's 138 kV transmission conductors are designed to carry the total output of the wind farm. As a result, the total load on the conductors was known and it was less likely that the conductors would be overloaded. Furthermore, the issue was short in duration, and occurred over a time period of four days in 2008.	Camp Grove reviewed and verified Facility Ratings for all equipment, including transmission conductors. In addition, Camp Grove reviewed and updated its procedure to address the Facility Rating requirements.

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*)	PPL Electric Utilities Corporation (PPL EU)	NCR00884	RFC2012001302	EOP-004-1	R3	On November 30, 2011, PPL EU, as a Load Serving Entity, submitted a Self-Report to Reliability*First* identifying an issue with EOP-004-1 R3. On November 30, 2011, PPL EU self-reported this issue via telephone. On January 6, 2012, PPL EU submitted a Self-Report form to Reliability*First.* PPL EU failed to provide a copy of the preliminary written report submitted to the U.S. Department of Energy (DOE) (Preliminary Report) to Reliability*First* and to NERC for one storm that resulted in a reportable incident pursuant to EOP-004-1, Attachment 2-EOP-004. During the last week of August 2011, PPL EU experienced a storm that resulted in loss of power to more than 50,000 customers for more than one hour. On August 28, 2011, PPL EU timely submitted the Preliminary Report to DOE; however, PPL EU failed to submit the Preliminary Report to Reliability*First* and NERC within 24 hours of the incident, as required by the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the risk was mitigated by the following factors. The reportable incident was storm-related, and PPL EU timely submitted the Preliminary Report to DOE. In addition, PPL EU's procedure states that submittals to DOE, NERC, and Reliability*First* are required, and PPL EU successfully implemented that procedure during events in May 2011 and October 2011. PPL EU's failure to provide the information to NERC and RFC was due to human error. In this instance, the individual responsible for submitting the report only submitted it to DOE, but not Reliability*First* and NERC. The statement that PPL EU successfully submitted reports to all necessary parties in May 2011 and October 2011 illustrates that PPL EU's procedure usually works, and that this was an isolated incident. Therefore, this remediated issue does not indicate a recurring issue at PPL EU.	In order to mitigate the remediated issue, PPL EU revised its procedure to contain a table of events and reporting requirements rather than a narrative explanation. PPL EU revised its operating instructions to refer to that procedure, rather than list the reporting requirements twice. In addition, PPL EU personnel reviewed the reporting requirements during a staff meeting. Furthermore, PPL EU added a review of the reporting requirements to its new operator training checklist to ensure all new operators understand their responsibilities regarding disturbance reporting.
Reliability*First* Corporation (Reliability*First)*	NRG Rockford LLC (NRG Rockford)	NCR06025	RFC2011001097	FAC-009-1	R1	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit of NRG Rockford (Compliance Audit). During the Compliance Audit, Reliability*First* determined NRG Rockford, as a Generator Owner (GO), did not establish Facility Ratings for its transmission line, breaker disconnect switch, and protective relay coils. During the Compliance Audit, Reliability*First* determined that while NRG Rockford had a column for normal and emergency ratings in its ratings table, it did not include those ratings under the associated column in its ratings table. NRG Rockford did include all normal ratings under a column in the ratings table titled "MVA/A/PF." Further, NRG Rockford's emergency ratings are identical to the normal ratings, which NRG Rockford included in the MVA/A/PF column of the ratings table.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). As a GO and Generator Operator, NRG Rockford designed all elements from the generator to the interconnection point to have a higher rating than the maximum output capability of the respective generating units. The most limiting element of NRG Rockford's facility is its respective generators. Following the Compliance Audit, NRG Rockford confirmed there were no current limitations that would result in the relays being a limiting element. Further, during the Compliance Audit, Reliability*First* found that, as the facility at issue was a generating station, the impact to the BPS by the omission of these devices was minimal since the loadability of the terminal equipment is limited by the generator capacity.	On November 22, 2011, NRG Rockford submitted additional information to Reliability*First* in which the NRG Rockford certified that it established Facility Ratings for the relay current coils and updated its respective Facility Ratings documentation to include the relay current coil ratings. NRG Rockford had provided Reliability*First* Facility Ratings for the transmission line and breaker disconnect switch prior to the completion of the Compliance Audit.
Reliability*First* Corporation (Reliability*First)*	NRG Rockford II LLC (NRG Rockford II)	NCR06024	RFC2011001100	FAC-009-1	R1	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit of NRG Rockford II (Compliance Audit). During the Compliance Audit, Reliability*First* determined NRG Rockford II, as a Generator Owner (GO), did not establish Facility Ratings for its transmission line, breaker disconnect switch, and protective relay coils. During the Compliance Audit, Reliability*First* determined that while NRG Rockford II had a column for normal and emergency ratings in its ratings table, they did not include those ratings under the associated column in its ratings table. NRG Rockford II did include all normal ratings under a column in the ratings table titled "MVA/A/PF." Further, NRG Rockford II's emergency ratings are identical to the normal ratings, which NRG Rockford II included in the MVA/A/PF column of the ratings table.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). As a GO and Generator Operator, NRG Rockford II designed all elements from the generator to the interconnection point to have a higher rating than the maximum output capability of the respective generating units. The most limiting element of NRG Rockford II's facility is its respective generators. Following the Compliance Audit, NRG Rockford II confirmed there were no current limitations that would result in the relays being a limiting element. Further, during the Compliance Audit, Reliability*First* found that, as the facility at issue was a generating station, the impact to the BPS by the omission of these devices was minimal since the loadability of the terminal equipment is limited by the generator capacity.	On November 22, 2011, NRG Rockford II submitted additional information to Reliability*First* in which the NRG Rockford II certified that it established Facility Ratings for the relay current coils and updated its respective Facility Ratings documentation to include the relay current coil ratings. NRG Rockford II had provided Reliability*First* Facility Ratings for the transmission line and breaker disconnect switch prior to the completion of the Compliance Audit.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	NRG Rockford LLC (NRG Rockford)	NCR06025	RFC2011001099	VAR-002-1.1a	R2	From July 11, 2011 through July 22, 2011, ReliabilityFirst conducted a compliance audit of NRG Rockford (Compliance Audit). During the Compliance Audit, Reliability*First* determined the NRG Rockford, as a Generator Operator, did not maintain its assigned voltage schedule, 141 kV +/- 2 kV. Specifically, on July 6, 2010, NRG Rockford's Unit 11 was under its voltage schedule by between 500 V and 2,500 V from approximately 2:00 p.m. until 7:00 p.m. On July 7, 2010, Unit 11 was under its voltage schedule by between 500 V and 2,500 V from approximately 11:00 a.m. until 4:35 p.m.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). NRG Rockford and NRG Rockford II (collectively, the NRG Entities) are located in the geographic middle of Commonwealth Edison Company's (ComEd') 138 kV system with limited ability to unilaterally raise system voltage. For example, on three of the four occasions for which Reliability*First* determined the NRG Entities operated outside their assigned voltage schedule, the respective NRG Entity was operating at maximum reactive power output. Although operating at maximum reactive power, the NRG Entities still remained below their assigned voltage schedule. In all three cases, the NRG Entities could not raise the reactive power output without risking thermal damage to the generating units. The NRG Entities' Interconnection Agreement with ComEd acknowledges that the NRG Entities have limited ability to strongly influence the ComEd system voltage at certain times. Additionally, Reliability*First* determined the NRG Entities were operating at less than 5% outside of their assigned voltage schedule on all four occasions. During the Compliance Audit, Reliability*First* determined that the impact on the BPS was minimal due to minimal running time and the limited impact of the affected machines on the local voltages.	On November 22, 2011, NRG Rockford submitted additional information to Reliability*First* in which NRG Rockford stated that on August 5, 2011, it conducted training sessions for its unit operators to notify ComEd when a unit reached maximum reactive output. On August 17, 2011, NRG Rockford also installed visual and audible voltage alarms to alert unit operators when voltage is off schedule.
Reliability*First* Corporation (Reliability*First)*	NRG Rockford II LLC (NRG Rockford II)	NCR06024	RFC2011001102	VAR-002-1.1a	R2	From July 11, 2011 through July 22, 2011, Reliability*First* conducted a compliance audit of NRG Rockford II (Compliance Audit). During the Compliance Audit, Reliability*First* determined NRG Rockford II, as a Generator Operator, did not maintain its assigned voltage schedule, 141 kV +/- 2 kV, on four separate occasions. On August 10, 2010 NRG Rockford II, LLC's Unit 21 (Unit 21) was under its voltage schedule by between 500 V and 2,000 V from approximately 12:30 p.m. until 9:00 p.m. On August 12, 2010, Unit 21 was under its voltage schedule by between 500 V and 2,000 V from approximately 11:20 a.m. until 6:15 p.m.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. NRG Rockford and NRG Rockford II (collectively, the NRG Entities) are located in the geographic middle of Commonwealth Edison Company's (ComEd's) 138 kV system with limited ability to unilaterally raise system voltage. For example, on three of the four occasions for which Reliability*First* determined the NRG Entities operated outside their assigned voltage schedule, the respective NRG Entity was operating at maximum reactive power output. Although operating at maximum reactive power, the NRG Entities still remained below their assigned voltage schedule. In all three cases, the NRG Entities could not raise the reactive power output without risking thermal damage to the generating units. The NRG Entities' Interconnection Agreement with ComEd acknowledges that the NRG Entities have limited ability to strongly influence the ComEd system voltage at certain times. Additionally, Reliability*First* determined the NRG Entities were operating at less than 5% outside of their assigned voltage schedule on all four occasions. During the Compliance Audit, Reliability*First* determined that the impact on the BPS was minimal due to minimal running time and the limited impact of the affected machines on the local voltages.	On November 22, 2011, NRG Rockford II submitted additional information to Reliability*First* in which NRG Rockford II stated that on August 5, 2011, it conducted training sessions for its unit operators to notify ComEd when a unit reached maximum reactive output. On August 17, 2011, NRG Rockford II also installed visual and audible voltage alarms to alert unit operators when voltage is off schedule.
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge Wind Farm LLC (Fowler Ridge)	NCR10307	RFC2012009876	FAC-008-1	R1; R1.2.1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III Wind Farm LLC (Fowler Ridge III), an affiliate of Fowler Ridge (Compliance Audit), during which Reliability*First* discovered an issue with FAC-008-1 R1. This issue also involved Fowler Ridge, which, with Fowler Ridge III, uses a common compliance program managed by AE Power. Reliability*First* determined that Fowler Ridge, as a Generator Owner, had an issue with the Standard for failing to include terminal equipment in its Facility Ratings Methodology.	ReliabilityFirst 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. Fowler Ridge reported that the most limiting element did not change as a result of updating the Facility Ratings Methodologies and Fowler Ridge has never de-rated a facility. The facility was also designed such that none of the equipment in Fowler Ridge's junction switchyard, which includes the terminal equipment at issue, could be the most limiting element.	On October 25, 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with FAC-008-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with FAC-008-1 R1. Fowler Ridge III revised its Facility Ratings Methodology to include terminal equipment. Fowler Ridge III also ensured that it identified and considered terminal equipment in its Facility Ratings. On November 29, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 28, 2011. Reliability*First* verified that the same mitigating actions were performed for Fowler Ridge and were completed as of November 28, 2011.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge Wind Farm LLC (Fowler Ridge)	NCR10307	RFC2012009877	PRC-005-1	R1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III Wind Farm LLC (Fowler Ridge III) (Compliance Audit), an affiliate of Fowler Ridge, during which Reliability*First* discovered an issue with PRC-005-1 R1. This issue alsoinvolved Fowler Ridge, which, with Fowler Ridge III, uses a common compliance program managed by AE Power. In its Protection System maintenance and testing program, Fowler Ridge failed to include its sole communications device associated with the Protection System, a power line carrier communications device, which constitutes 1 of its 54 (1.85%) total Protection System devices. Reliability*First* determined that Fowler Ridge, as a Generator Owner, had an issue with the Standard for failing to include: (a) maintenance and testing interval and basis for that interval; and (b) summary of maintenance and testing procedures for this device in its Protection System maintenance and testing program.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The communications device at issue, which is located in the junction switchyard shared and jointly owned by Fowler Ridge, is continuously monitored via an alarm that is triggered if the system detects a communications error or other improper operation. This alarm sends a message to a wind farm event alarm screen, which is located and monitored in the Remote Operations Center, a staffed facility located in Houston, Texas that is responsible for addressing real-time emergency conditions and is also the point of contact for reliability issues for Fowler Ridge. Additionally, Fowler Ridge tested the communications device during plant commissioning in October 2008, which was within its testing and maintenance schedule at the time of the Compliance Audit; therefore, this constitutes a documentation-only issue.	On October 28 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with of PRC-005-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with PRC-005-1 R1. AE Power, the entity responsible for maintaining Fowler Ridge III's compliance program, revised its Protection System procedures, including those for associated communications equipment, and implemented a new procedure on November 30, 2011. This procedure includes maintenance and testing intervals, basis for the intervals, and a summary of maintenance and testing procedures for associated communication systems. On December 1, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 30, 2011. On February 8, 2012, Reliability*First* verified this completion. Reliability*First* also verified that the same mitigating actions were performed for Fowler Ridge and were completed as of November 30, 2011.
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge II Wind Farm LLC (Fowler Ridge II)	NCR03040	RFC2012009878	FAC-008-1	R1; R1.2.1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III Wind Farm LLC (Fowler Ridge III), an affiliate of Fowler Ridge II (Compliance Audit), during which Reliability*First* discovered an issue with FAC-008-1 R1. This issue also involved Fowler Ridge II, which, with Fowler Ridge III, uses a common compliance program managed by AE Power. Reliability*First* determined that Fowler Ridge II, as a Generator Owner, had an issue with the Standard for failing to include terminal equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Fowler Ridge II reported that the most limiting element did not change as a result of updating the Facility Ratings Methodologies and Fowler Ridge II has never de-rated a facility. The facility was also designed such that none of the equipment in Fowler Ridge II's junction switchyard, which includes the terminal equipment at issue, could be the most limiting element.	On October 25, 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with FAC-008-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with FAC-008-1 R1. Fowler Ridge III revised its Facility Ratings Methodology to include terminal equipment. Fowler Ridge III also ensured that it identified and considered terminal equipment in its Facility Ratings. On November 29, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 28, 2011. Reliability*First* verified that the same mitigating actions were performed for Fowler Ridge II and were completed as of November 28, 2011.
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge II Wind Farm LLC (Fowler Ridge II)	NCR03040	RFC2012009879	PRC-005-1	R1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III Wind Farm LLC (Fowler Ridge III) (Compliance Audit), an affiliate of Fowler Ridge II, during which Reliability*First* discovered an issue with PRC-005-1 R1. This issue also involved Fowler Ridge II, which, with Fowler Ridge III, uses a common compliance program managed by AE Power. In its Protection System maintenance and testing program, Fowler Ridge II failed to include its sole communications device associated with the Protection System, a power line carrier communications device, which constitutes 1 of its 54 (1.85%) total Protection System devices. Reliability*First* determined that Fowler Ridge II, as a Generator Owner, had an issue with the Standard for failing to include: (a) maintenance and testing interval and basis for that interval; and (b) summary of maintenance and testing procedures for this device in its Protection System maintenance and testing program.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The communications device at issue, which is located in the junction switchyard shared and jointly owned by Fowler Ridge II is continuously monitored via an alarm that is triggered if the system detects a communications error or other improper operation. This alarm sends a message to a wind farm event alarm screen, which is located and monitored in the Remote Operations Center, a staffed facility located in Houston, Texas that is responsible for addressing real-time emergency conditions and is also the point of contact for reliability issues for Fowler Ridge II. Additionally, Fowler Ridge II tested the communications device during plant commissioning in October 2008, which was within its testing and maintenance schedule at the time of the Compliance Audit; therefore, this constitutes a documentation-only issue.	On October 28 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with PRC-005-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with PRC-005-1 R1. AE Power, the entity responsible for maintaining Fowler Ridge III's compliance program, revised its Protection System procedures, including those for associated communications equipment, and implemented a new procedure on November 30, 2011. This procedure includes maintenance and testing intervals, basis for the intervals, and a summary of maintenance and testing procedures for associated communication systems. On December 1, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 30, 2011. On February 8, 2012, Reliability*First* verified this completion. Reliability*First* also verified that the same mitigating actions were performed for Fowler Ridge II and were completed as of November 30, 2011.
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge III Wind Farm LLC (Fowler Ridge III)	NCR10308	RFC201100993	FAC-008-1	R1; R1.2.1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III (Compliance Audit). During the Compliance Audit, Reliability*First* discovered an issue with FAC-008-1 R1. Reliability*First* determined that Fowler Ridge III, as a Generator Owner, had an issue with the Standard for failing to include terminal equipment in its Facility Ratings Methodology.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. Fowler Ridge III reported that the most limiting element did not change as a result of updating the Facility Ratings Methodologies and Fowler Ridge III has never de-rated a facility. The facility was also designed such that none of the equipment in Fowler Ridge III's junction switchyard, which includes the terminal equipment at issue, could be the most limiting element.	On October 25, 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with FAC-008-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with FAC-008-1 R1. Fowler Ridge III revised its Facility Ratings Methodology to include terminal equipment. Fowler Ridge III also ensured that it identified and considered terminal equipment in its Facility Ratings. On November 29, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 28, 2011. On January 25, 2012, Reliability*First* verified this completion.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Fowler Ridge III Wind Farm LLC (Fowler Ridge III)	NCR10308	RFC201100994	PRC-005-1	R1	From May 2, 2011 through May 17, 2011, Reliability*First* conducted a compliance audit of Fowler Ridge III (Compliance Audit). During the Compliance Audit, Reliability*First* discovered an issue with PRC-005-1 R1. In its Protection System maintenance and testing program, Fowler Ridge III failed to include its sole communications device associated with the Protection System, a power line carrier communications device, which constitutes 1 of its 54 (1.85%) total Protection System devices. Reliability*First* determined that Fowler Ridge II, as a Generator Owner, had an issue with the Standard for failing to include: (a) maintenance and testing interval and basis for that interval; and (b) summary of maintenance and testing procedures for this device in its Protection System maintenance and testing program.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The communications device at issue, which is located in the junction switchyard shared and jointly owned by Fowler Ridge III is continuously monitored via an alarm that is triggered if the system detects a communications error or other improper operation. This alarm sends a message to a wind farm event alarm screen, which is located and monitored in the Remote Operations Center, a staffed facility located in Houston, Texas that is responsible for addressing real-time emergency conditions and is also the point of contact for reliability issues for Fowler Ridge III. Additionally, Fowler Ridge III tested the communications device during plant commissioning in October 2008 that would have been within its testing and maintenance schedule at the time of the Compliance Audit; therefore, this constitutes a documentation-only issue.	On October 28 2011, Fowler Ridge III submitted to Reliability*First* a Mitigation Plan to address the issue with PRC-005-1 R1. In this Mitigation Plan, Fowler Ridge III memorialized the actions it took to address the issue with PRC-005-1 R1. AE Power, the entity responsible for maintaining Fowler Ridge III's compliance program, revised its Protection System procedures, including those for associated communications equipment, and implemented a new procedure on November 30, 2011. This procedure includes maintenance and testing intervals, basis for the intervals, and a summary of maintenance and testing procedures for associated communication systems. On December 1, 2011, Fowler Ridge III stated that it completed its Mitigation Plan as of November 30, 2011. On February 8, 2012, Reliability*First* verified this completion.
SERC Reliability Corporation (SERC)	Virginia Electric and Power Company (DP, LSE, TO) (VEPCO)	NCR01214	SERC2011007878	FAC-008-1	R1	VEPCO, as a Transmission Owner (TO), self-reported a possible issue with FAC-008-1 R1, stating that it had identified a failure to include a rating methodology for circuit switchers in its Facility Rating Methodology (FRM). SERC staff reviewed two versions of VEPCO's FRM. VEPCO's 2007 FRM was in effect at the time FAC-008-1 became enforceable. VEPCO's 2010 FRM was in effect when VEPCO submitted its Self-Report to SERC. After reviewing these documents, SERC staff determined that both versions failed to include a Methodology for rating circuit switchers. SERC staff also determined that both versions of the FRM failed to address series compensation devices. SERC staff found no other issues with VEPCO's FRMs.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The circuit switchers are not the most limiting components in VEPCO's Facility Ratings and therefore VEPCO's failure to include them in its FRM did not affect the determination of the Facility Rating; 2. The circuit switchers were installed at only nine out of 200 VEPCO substations; and 3. VEPCO did not use series compensation devices and therefore its failure to include those devices in its FRM did not affect the determination of the Facility Rating.	SERC staff verified that VEPCO completed the following actions: 1. VEPCO developed a circuit switcher rating methodology (CSRM) as an interim measure until the accuracy of the CSRM could be verified by the circuit switcher's manufacturer. In addition, VEPCO conducted a thorough assessment and determined that the circuit switchers were never the most limiting element from a facility ratings perspective; 2. Upon verification of accuracy by the circuit switcher's manufacturer, VEPCO's CSRM was finalized and incorporated into VEPCO's revised FRM; 3. VEPCO included language in its revised FRM to specifically address Transmission Series Compensation Devices; and 4. VEPCO finalized its revised FRM.
SERC Reliability Corporation (SERC)	Virginia Electric and Power Company (DP, LSE, TO) (VEPCO)	NCR01214	SERC2011008221	NUC-001-2	R4	VEPCO, as a Transmission Owner, self-reported a possible issue with NUC-001-2 R4. VEPCO lost the ability to assess the operation of the electric system affecting the Nuclear Plant Interface Requirements (NPIRs) and did not contact the Nuclear Power Generator Operators (NPG Operators) within 15 minutes as required by the Nuclear Switchyard Interface Agreement (NSIA). Two stations were affected. The incident occurred on November 6, 2010. SERC staff reviewed the NSIA, which affects the NPIRs. The NSIA Agreement requires VEPCO to notify the stations within 15 minutes when certain systems are known to be out of service. According to the operator log book from November 6, 2010, at 10:03 a.m. the IT duty person was alerted to a computer issue affecting VEPCO's Energy Management System (EMS) via an automatic page. At 10:12 a.m., the System Operations Center (SOC) Supervisor informed the Reliability Coordinator and Transmission Operator that VEPCO lost the ability to assess the operation of the electric system affecting the NPIRs but did not notify the NPG Operators until 10:57 a.m. and 10:59 a.m., respectively. At 11:09 a.m., the ability to assess the operation of the electric system affecting the NPIRs was restored. The issue with the EMS was caused by a processor malfunction that caused the computer to run so slowly that it appeared to be down, but never stopping completely, which prevented the primary computer from failing over to the standby computer, as designed. Once the nature of this problem was identified, the malfunction was promptly corrected.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The NPG Operators were still monitoring the stations and were responsible for addressing any alarms that may have arisen; 2. The NPG Operators were notified within the hour; and 3. The EMS issue was corrected within 66 minutes.	SERC staff verified that VEPCO completed the following actions: 1. Installed an alarm mechanism on the EMS system at the application level that alerts the SOC Supervisor when EMS applications stall; and 2. Provided additional SOC supervisor training regarding the communication requirements defined in the NPIRs.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
SERC Reliability Corporation (SERC)	Big Rivers Electric Corporation (BREC)	NCR01180	SERC2011007289	PRC-005-1	R1	On April 6, 2011, SERC sent BREC a notice of an on-site Spot Check of Reliability Standard PRC-005-1 . On May 24, 2011, the SERC Spot Check Team reported a possible violation of PRC-005-1 R1 because BREC's Protection System maintenance and testing program for its Generator Owner (GO) and Transmission Owner (TO) functions did not address the basis for the maintenance and testing intervals for associated communications systems, voltage and current sensing devices, and DC control circuitry. SERC staff reviewed the procedures in effect at the beginning of the enforceable period. Three documents comprised the Protection System maintenance and testing program. The basis for the maintenance and testing intervals was not included for associated communications systems, voltage and current sensing devices, and DC control circuitry. SERC staff reviewed the Protection System maintenance and testing procedure that became effective on June 30, 2008. This version meets all of the elements of PRC-005-1 R1.	SERC staff determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. The issue was due to a gap in documentation for the BREC Protection System maintenance and testing program from June 18, 2007 until June 30, 2008; and 2. Maintenance and testing was being conducted for these elements during the audit scope time line.	SERC staff verified that BREC completed the following actions: 1. Amended its Protection System maintenance and testing program to reflect the basis for associated communication systems, voltage and current sensing devices, and DC control circuitry.
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100618	CIP-001-1	R1	During a June 8, 2011 to June 9, 2011 Compliance Audit, SPP RE discovered that Gardner, as a Load Serving Entity (LSE), did not have a Sabotage Reporting procedure for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi-site sabotage affecting larger portions of the Interconnection, as required by CIP-001-1 R1. SPP RE determined that the issue was from December 20, 2007, when Gardner was registered as a LSE, through December 31, 2008, the date in which Gardner implemented a Sabotage Reporting procedure.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Gardner is a small municipal electric utility with a generation capacity of 30 MW (two generating units with an MVA rating of 15 each); 3.6 miles of radial 161 kV transmission lines; terminal equipment at a substation owned by another Registered Entity; and fewer than 7,000 electric customers. Due to Gardner's small size and insignificant ownership interest in the BPS any sabotage of the Gardner system would have minimal impact on the BPS. Furthermore, the period in which Gardner did not have a Sabotage Reporting procedure was limited to one year. Finally, Gardner did not have any Critical Assets or Critical Cyber Assets, which further reduced the risk to the BPS.	Gardner created a Sabotage Reporting procedure on December 31, 2008 that addressed the requirements listed in CIP-001-1. All subsequent revisions to Gardner's Sabotage Reporting procedure have also addressed the requirements of CIP-001-1 R1.
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100619	CIP-001-1	R2	During a June 8, 2011 to June 9, 2011 Compliance Audit, SPP RE discovered that Gardner, as a Load Serving Entity (LSE), did not have a Sabotage Reporting procedure for the communication of information concerning sabotage events to appropriate parties in the Interconnection, as required by CIP-001-1 R2. SPP RE determined this issue was from December 20, 2007, when Gardner was registered as a LSE, through December 31, 2008, the date in which Gardner implemented a Sabotage Reporting procedure.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Gardner is a small municipal electric utility with a generation capacity of 30 MW (two generating units with an MVA rating of 15 each); 3.6 miles of radial 161 kV transmission lines; terminal equipment at a substation owned by another Registered Entity; and fewer than 7,000 electric customers. Due to Gardner's small size and insignificant ownership interest in the BPS any sabotage of the Gardner system would have minimal impact on the BPS. Furthermore, the period in which Gardner did not have a Sabotage Reporting procedure was limited to one year. Finally, Gardner did not have any Critical Assets or Critical Cyber Assets, which further reduced the risk to the BPS.	Gardner created a Sabotage Reporting procedure on December 31, 2008 that addressed the requirements listed in CIP-001-1. All subsequent revisions to Gardner's Sabotage Reporting procedure have also addressed the requirements of CIP-001-1 R2.
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100620	CIP-001-1	R3	During a June 8, 2011 to June 9, 2011 Compliance Audit, SPP RE discovered that Gardner, as a Load Serving Entity (LSE), did not have a Sabotage Reporting procedure that provided Gardner's operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events, as required by CIP-001-1 R2. SPP RE determined that the issue was from December 20, 2007, when Gardner was registered as a LSE, through December 31, 2008, the date in which Gardner implemented a Sabotage Reporting procedure.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Gardner is a small municipal electric utility with a generation capacity of 30 MW (two generating units with an MVA rating of 15 each); 3.6 miles of radial 161 kV transmission lines; terminal equipment at a substation owned by another Registered Entity; and fewer than 7,000 electric customers. Due to Gardner's small size and insignificant ownership interest in the BPS any sabotage of the Gardner system would have minimal impact on the BPS. Furthermore, the period in which Gardner did not have a Sabotage Reporting procedure was limited to one year. Finally, Gardner did not have any Critical Assets or Critical Cyber Assets, which further reduced the risk to the BPS.	Gardner created a Sabotage Reporting procedure on December 31, 2008 that addressed the requirements listed in CIP-001-1. All subsequent revisions to Gardner's Sabotage Reporting procedure have also addressed the requirements of CIP-001-1 R3.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Southwest Power Pool Regional Entity (SPP RE)	City of Gardner (Gardner)	NCR10190	SPP201100621	CIP-001-1	R4	During a June 8, 2011 to June 9, 2011 Compliance Audit, SPP RE discovered that Gardner, as a Load Serving Entity (LSE), did not have a Sabotage Reporting procedure that established communications contacts with local Federal Bureau of Investigation (FBI) officials and developed reporting procedures as appropriate to their circumstances, as required by CIP-001-1 R4. SPP RE determined that the issue was from December 20, 2007, when Gardner was registered as a LSE, through December 31, 2008, the date in which Gardner implemented a Sabotage Reporting procedure.	SPP RE determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Gardner is a small municipal electric utility with a generation capacity of 30 MW (two generating units with an MVA rating of 15 each); 3.6 miles of radial 161 kV transmission lines; terminal equipment at a substation owned by another Registered Entity; and fewer than 7,000 electric customers. Due to Gardner's small size and insignificant ownership interest in the BPS any sabotage of the Gardner system would have minimal impact on the BPS. Furthermore, the period in which Gardner did not have a Sabotage Reporting procedure was limited to one year. Finally, Gardner did not have any Critical Assets or Critical Cyber Assets, which further reduced the risk to the BPS.	Gardner created a Sabotage Reporting procedure on December 31, 2008 that addressed the requirements listed in CIP-001-1. All subsequent revisions to Gardner's Sabotage Reporting procedure have also addressed the requirements of CIP-001-1 R4.
Southwest Power Pool Regional Entity (SPP RE)	PowerSmith Cogeneration Project, LP (Powersmith)	NCR11119	SPP201100651	CIP-001-1a	R2	On July 31, 2011, Powersmith, as a Generator Operator, self reported a possible issue with CIP-001-1 R2. Prior to Powersmith registering with SPP RE on April 22, 2011, Powersmith had a Sabotage Reporting procedure in place. However, Powersmith's Sabotage Reporting procedure did not include all appropriate parties in the Interconnection that Powersmith should communicate information concerning sabotage events. In particular, Powersmith did not include its Transmission Operator (TOP) as an appropriate party, as required by CIP-001-1 R2.	SPP RE determined that the issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Powersmith did have a Sabotage Reporting procedure in place at the time it registered with SPP RE and the Sabotage Reporting procedure satisfied CIP-001-1 R1, R3 and R4. Therefore, if a sabotage were to occur, Powersmith's employees would have known how to react to the sabotage event. Also, Powersmith did have its Reliability Coordinator and Balancing Authority listed as appropriate parties to communicate with concerning sabotage events and only failed to include its TOP as an appropriate party.	On August 25, 2011, Powersmith revised its Sabotage Reporting procedure to include its TOP as an appropriate party in the interconnection as a party to communicate with concerning sabotage events.
Southwest Power Pool Regional Entity (SPP RE)	PowerSmith Cogeneration Project, LP (Powersmith)	NCR11119	SPP201100658	TOP-002-2a	R18	On July 31, 2011, Powersmith, as a Generator Operator, self-reported a possible issue with TOP-002-2a R18 for failure to use uniform line identifiers when referring to transmission facilities of an interconnected network. Powersmith reported that it had not identified its transmission line to Oklahoma Gas And Electric Co.'s (OG&E's) Dayton Substation in a way that would be uniform with the name that OG&E had assigned to the line connecting the Powersmith's generator with OG&E. The name assigned by OG&E was "Dayton to Smith Co-generation Inc. 138 kV line."	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). The transmission line from Powersmith to OG&E is Powersmith's only interconnection with OG&E and was only 455 feet in length. Furthermore, the interconnection ties directly to an OG&E substation (Dayton) and does not have any intermediate ties or connections to other OG&E facilities. Additionally, Powersmith began using the OG&E line identifier for the referenced line within five-months of its NERC registration. SPP RE determined the potential for miscommunications regarding the interconnection was improbable because the tie is Powersmith's only interconnection with OG&E.	Powersmith established a uniform transmission line identification with OG&E's substation and placed the uniform identification on its Station Drawings.

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)	Red Hills Wind Project, LLC. (RHWP)	NCR10304	SPP2011008532	PRC-001-1	R3	On November 14, 2011, RHWP self-reported a possible issue with PRC-001-1 R3. RHWP stated that on August 24, 2011, RHWP made a temporary change to the pickup point of its time delay overcurrent relay (ANSI 51) from 2400A to 1600A after experiencing a failure of its 34.5 kV main circuit breaker. The pickup point change was required because the spare circuit breaker, which was placed in service by RHWP, had a lower current rating (1600A) than the failed (2400A) breaker. This change was coordinated with Western Farmers Electrical Cooperative (WFEC), RHWP's Transmission Operator (TOP) and host Balancing Authority (BA). WFEC was informed this was only a temporary change due to the breaker failure. RHWP informed WFEC it anticipated receiving a replacement (2400A) breaker by August 29, 2011. On August 30, 2011, RHWP initiated a maintenance outage, which was coordinated with WFEC and the Southwest Power Pool, Reliability Coordinator (SPP RC) to replace the breaker that failed on August 24, 2011. During the maintenance outage, RHWP returned the pickup point of the time delay overcurrent relay (ANSI 51) to the original set point of 2400A. This change was not coordinated with WFEC prior to bringing RHWP's facility on line at approximately 3:00 p.m. on August 30, 2011. On August 31, 2011 at approximately 8:33 a.m., RHWP notified WFEC of the change to the pickup point of the time delay overcurrent relay (ANSI 51) back to the original set point of 2400A. On September 2, 2011, RHWP received a written correspondence from WFEC that the change made to the pickup point of the time delay overcurrent relay did not require WFEC to make changes on its system. SPP RE determined that RHWP, as a Generator Operator, failed to coordinate all new protective systems and changes with its TOP and BA, as required by PRC-001-1 R3.	SPP RE determined that RHWP's issue with PRC-001-1 R3 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). RHWP's change to the overcurrent relay pickup point of the main breaker from 2400A to 1600A was temporary, and WFEC was informed that RHWP anticipated permanently replacing the main circuit breaker (rated for 2400A) by August 29, 2011, one day before the coordinated outage. RHWP failed only to communicate to WFEC that it was changing the pickup point back to 2400A. RHWP did, however, communicate with WFEC and SPP RC, regarding its breaker failure; the disconnection and reconnection of RHWP's facility; and RHWP's ability to reach full production capability. Additionally, WFEC indicated that the change to the pickup point of the overcurrent relay did not impact WFEC's transmission system.	RHWP has undertaken the following activities to correct its noncompliance with PRC-001-1 R3: • On September 7, 2011, the AENA Director, Operations & Maintenance discussed with the RHWP's maintenance personnel RHWP's potential noncompliance with PRC-001-1 R3 and reinforced the requirement to coordinate all protection system changes with the TOP and BA. • On September 21, 2011, the Regulatory Compliance Analyst presented to RHWP maintenance personnel a Regulatory Compliance Strategic Analysis on NERC Abbreviated Notice of Penalty that included discussion of PRC-001-1 R3 violations. This strategic analysis also included a discussion of the events that occurred at RHWP on August 30, 2011. • Regulatory Compliance training was provided to RHWP maintenance personnel on October 5, 2011 and October 10, 2011, which included training on AENA Standard PRC-001-1 System Protection Coordination and a discussion of RHWP's noncompliance with PRC-001-1 R3 to ensure that AENA generation facilities are in compliance with the applicable NERC standards.
Texas Reliability Entity, Inc. (Texas RE)	Horse Hollow Generation Tie, LLC (HHGT)	NCR10392	TRE201000173	PER-003-0	R1	In connection with its registration as a Transmission Operator (TOP), HHGT submitted a TOP Implementation Plan to Texas RE, stating that HHGT's operators would be NERC-certified by December 1, 2010. The purpose of the Implementation Plan was to address certain deficiencies HHGT identified in preparation for its TOP certification review. Prior to its TOP registration, HHGT was not required to staff its operating positions with NERC-certified operators. HHGT self-reported that, on the date of its registration as a TOP, one out of four transmission operators were NERC-certified. Texas RE determined that HHGT had an issue with PER-003-0 R1 because three operators did not have the requisite NERC certification. The duration of this issue was from September 19, 2010, the date HHGT was registered as a TOP, through December 18, 2010, when all of HHGT's operators were NERC-certified.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was mitigated by several factors. First, Texas RE determined that although three of HHGT's operators were not NERC-certified of the previous experience of the HHGT operators in performing transmission operation functions and the procedures that were implemented with the Electric Reliability Council of Texas, Inc. (ERCOT) prior to becoming a NERC registered Transmission Operator. Second, several procedures that reduced the risk to the BPS were implemented with the ERCOT prior to HHGT becoming a NERC registered TOP. These procedures required HHGT to send a week-ahead Work Plan to ERCOT every Friday, which included the status of all equipment affecting the power flow on the HHGT 345 kV line and the line capability. Forced outages and information impacting real-time operations were also communicated immediately to the ERCOT shift supervisor with a follow-up email. Day-ahead changes were shared with the Operations Support Engineering Group and the ERCOT Shift Engineer, real-time operational data was sent to ERCOT via a current NextEra Energy Resources data link, and any sabotage reporting involving the HHGT 345 kV line or substations was sent via email to the ERCOT shift supervisor.	To mitigate the issue, HHGT added three NERC-certified transmission operators to its staff. Texas RE verified with NERC that the operators held NERC certifications.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Arizona Public Service Company (AZPS)	NCR05016	WECC2011008672	VAR-002-1.1b	R3	AZPS, as a Generator Operator, submitted a Self-Report to WECC stating that on October 9, 2011, at 9:12 AZPS's Palo Verde (PV) Nuclear Generating Station Unit 3 (PV3) received an alarm caused by the Power System Stabilizer (PSS) comparator tripping. The PSS was reset by the GOP at 9:35, the alarm cleared, and the PSS returned to operation. The following day, at 12:30 AZPS performed a Control Board walk-down that noted that the PV3 PSS was taken out of service the previous day without notifying the Transmission Operator (TOP) within 30 minutes of the expected duration and the change in status. Although the GOP followed PV's Nuclear Administrative and Technical Manual Procedure the previous day by completing the Out-of-Service Report for the PV3 PSS, the operator failed to complete the notification process by failing to notify the Energy Control Center (ECC) of any change in status of the PSS within 30 minutes. As a result, AZPS's ECC was not notified of the PSS change in status until 24 hours later when the Control Board walk-down revealed the inconsistency in the process. Consequently, AZPS's TOP (EEC) was notified of the PV3 PSS change in status on October 10, 2011 by 12:30.	AZPS system conditions on Sunday, October 9, 2011, and Monday October 10, 2011 were stable and load conditions were low. AZPS has 56 generating units with a combined generating capacity of approximately 7217 MW. Of the 56 units, 21 units were in operation on October 9, 2011. During the time the PV3 PSS was out of service, the PSS equipment on all other PSS units was still operating. Therefore these remaining 20 units would have been able to respond to a system deviation. For these reasons, WECC determined this issue posed minimal risk to the bulk power system.	Upon discovery, AZPS notified the EEC of the change in status of the PSS on October 10, 2011 at 12:30. On October 14, 2011, PV management issued a Standing Order to all PV GOPs, that provided interim guidance until the procedure was updated, to reinforce the 30-minute notification requirement associated with any change in status of the PSS. The Standing Order required all on-duty, scheduled PV GOPs to review and acknowledge the instruction prior to commencing their next shift. Those operators not on active duty will be updated through the updated procedure upon their return to work. On October 17, 2011, AZPS' fossil generation duty officer advised all plant managers of the October 9, 2011 PV3 Self-Report and required face-to-face meetings with all GOPs be conducted by October 25, 2011. This action was taken in an effort to remind and reinforce to all generator operators the 30-minute notification requirement associated with any change in status of a PSS.
Western Electricity Coordinating Council (WECC)	Bonneville Power Administration (BPA)	NCR05032	WECC2011008664	MOD-010-0	R2	On March 24, 2011, BPA, as a Transmission Owner, Transmission Planner, and Resource Planner, received a request from a member of the planning staff of an adjacent entity, to provide steady-state modeling and simulation data. BPA provided the information to the requesting entity on April 25, 2011, thirty-two (32) days after the request was received. BPA was required by the Standard to have provided this data within thirty (30) days of the request.	WECC determined this issue posed minimal risk to the reliability of the bulk power system (BPS) because BPA responded to the entity request within 32 days instead of thirty days. Also, BPA did provide the requested information. A lapse of 2 days poses a minimal risk to the BPS because the delay did not affect the timing of the analysis.	BPA revised internal procedures for the receipt and response to requests made under MOD-010-0 R2 to include internal controls to ensure that BPA responds to an entity within 30 days of the request as required by the Standard.
Western Electricity Coordinating Council (WECC)	High Desert Power Project, LLC (HDPP)	NCR05184	WECC2012009132	VAR-002-1.1b	R3	HDPP, as a Generator Operator, submitted a Self-Report to WECC stating that on November 17, 2011 at 16:20, following a maintenance outage, HDPP started its combustion turbine unit 1 without turning the Power System Stabilizer (PSS) on. On November 20, 2011 the control room operator discovered the PSS in the off position, where it was left subsequent to the maintenance outage. On November 20, 2011 at 07:00 the PSS on combustion turbine unit 1 was put back in service, however, the plant operator failed to communicate this change in status to the Transmission Operator (TOP). On December 20, 2011, during a monthly review of the control room log books the change in status notification failure was discovered. As a result of this review, HDPP notified the TOP of the PSS change in status on December 20, 2011.	The unit operated with the PSS out of service for approximately 63 hours. During the time the PSS was turned off the automatic voltage regulator (AVR) was in service, reducing the probability of instability, thus reducing the probability of an unnecessary loss of a facility during an event. Furthermore, because the AVR was in service the entire time the PSS was turned off, the generator could still effectively respond to any voltage deviation. For these reasons, WECC determined this issue posed a minimal risk to the reliability of the bulk power system.	Upon discovery, HDPP notified the TOP of the change in status of the PSS. The plant operators were retrained on the NERC requirements for this Standard. An alarm was added to the plant control system to indicate that the PSS or the AVR were in the off position for the combustion turbines.
Western Electricity Coordinating Council (WECC)	High Desert Power Project, LLC (HDPP)	NCR05184	WECC2012009813	VAR-501-WECC-1	R1	HDPP, as a Generator Operator, submitted a Self-Report to WECC stating that on November 17, 2011 at 16:20, following a maintenance outage, HDPP started its combustion turbine unit 1 without turning the Power System Stabilizer (PSS) on. On November 20, 2011 at 07:00 the control room operator discovered the PSS in the off position and immediately turned the power stabilizer on. The total time the PSS was turned off for the fourth quarter 2011 was 62.6 hours. The total run time for the unit during the fourth quarter 2011 was 996.18 hours. Therefore, the PSS was in service for 93.7% of the operating time for the fourth quarter, which falls below the 98% threshold.	The unit operated with the PSS in service for the majority of the calendar quarter, reducing the probability of instability, thus reducing the probability of an unnecessary loss of a facility during an event. In addition, the automatic voltage regulator (AVR) was in service the entire time the PSS was turned off therefore ensuring the generator could respond effectively to any voltage deviations. For these reasons, WECC determined this issue posed a minimal risk to the reliability of the bulk power system.	HDPP returned the PSS to service and retrained the plant operators on PSS display information. Additionally, HDPP added an alarm to the plant control system to indicate that the PSS or the AVR are in the off position for the combustion turbine units.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Wood Group Power Operations (WGCS)	NCR10349	WECC2012009654	VAR-002-1.1b	R3	WGCS, as a Generator Operator, submitted a Self-Report to WECC stating that on January 22, 2012 at 21:38 hours, power from Pacific Gas and Electric Company's (PG&E's) substation to WGCS's Panoche Energy Center (PEC) was lost. To save batteries and control systems the PEC shut down its four generating units. On January 23, 2012 at 04:55 hours power was restored. WGCS proceeded to activate the PEC systems which included powering up the controls used for operating the four generating units. Specifically, PEC restored the Automatic Voltage Regulator (AVR) on Unit 4 at 06:04, Unit 3 at 06:06, Unit 2 at 06:10, and Unit 1 at 06:14. Two days later the operator performed a review of the units and discovered the Power System Stabilizer (PSS) was not enabled and the TOP was not notified of this change in status. As a result, WGCS immediately enabled the PSS on the four units and notified the Transmission Operator (TOP) (PG&E) of the PSS change in status on January 25, 2012.	PEC is a 400 MW simple-cycle power plant encompassing four 100 MW gas turbine generating units. The time the PSS was disabled the AVR on all units was still operating at 50 MW each. Therefore the units would be able to respond to any system deviation. In addition, these units are not base load units but a peaking facility dispatched by PG&E. For these reasons, WECC determined this issue posed minimal risk to the bulk power system.	Upon discovery, WGCS notified the TOP of the change in status of the PSS. WGCS also performed the following tasks to prevent reoccurrence: (1) installed a system through the plant's PI historian to e-mail all plant personnel plus the asset manager and regional WGCS project manager, whenever the PSS is disabled; (2) performed remedial training for the operators on the PSS system; (3) created and added a quick reference reporting card to the emergency ops book in the control room.

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	FRCC2011007977	CIP-004-3	R3	FRCC_URE1 self-reported that it failed to conduct personnel risk assessments (PRAs) for one of its personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, as required by CIP-004-3 R3. FRCC_URE1 granted remote access to the contractor at issue but did not conduct a PRA and document the results prior to granting access. This issue involved only one person, a contractor who accessed Critical Cyber Assets (CCAs) on three separate occasions for very short durations.	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 person accessed the systems for specific maintenance pursuant to a trusted vendor contract with complete direction from the plant system operator. The turbine tuning activities involved coordination of plant and vendor remote staff to acquire and analyze real-time dynamics data using locally-installed equipment. The remote user has no access to the local device so they have to coordinate in order to complete the exercise. Further, all recommendations are implemented after full consultation with the plant operations management. On all the three occasions, access was for short durations (less than 2 hours) and system access was monitored and all activities were performed with consultation and clear direction. Further, the vendor has performed this maintenance activity for the past six years for many large generating units and was used frequently as a trusted resource specializing in the activity. Although FRCC_URE1 has violated this Standard previously, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation appropriately. The prior violations involved on-site personnel, whereas the instant issue involved contractors accessing the assets remotely. Additionally, unlike the prior violations, the instant issue did not involve any new access provisioning, but rather, involved a contractual obligation with an existing vendor . This access was not a planned exercise but an unplanned usage of an access path that was scarcely used. Further, this instance was related to different controls and a different compliance schedule than in the prior violations, which involved the control center.	FRCC_URE1 certified that it completed its mitigation activities by revoking access and creating a new procedure for on-boarding all new vendor contractors that access systems remotely, which requires FRCC_URE1 to conduct PRAs and training prior to granting access to any CCAs and training of all personnel responsible for granting access to CCAs.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC2011008234	CIP-005-1	R1; R1.6	During a NERC CIP Compliance Audit, it was determined that FRCC_URE1 failed to document one of the Cyber Assets that is used to configure the intrusion detection system and hence perform electronic access control and monitoring, as required by CIP-005-1 R1.6. The Cyber Asset was not included on the Cyber Assets inventory list for a period of approximately a year and a half. FRCC_URE1 continued to provide the required CIP protection but failed to document the devices on its list of Cyber Assets as an Electronic Access Control and Monitoring (EACM) System.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because even though the device was not documented on its Cyber Assets inventory list, it was within the Electronic Security Perimeter and afforded protective measures as required by CIP-005 R1.5. This issue occurred because prior to the Audit, FRCC_URE1 did not understand that devices used to configure EACMs were required to be considered EACMs for purposes of the Cyber Assets inventory list. Although FRCC_URE1 has violated this Standard previously, the instant remediated issue is appropriate for FFT treatment because it does not represent a failure to mitigate a prior violation appropriately. The prior violations involved identification of non-Critical Cyber Assets (R1.4), whereas this issue was related to protection of the EACM system (R1.6). Though both subrequirements are part of CIP-005 R1, they are distinct with separate security controls, control measures, and control owners.	FRCC_URE1 certified that it completed its mitigation activities by correcting the list of electronic access control and monitoring systems to include the intrusion detection system asset.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 1 (FRCC_URE1)	NCRXXXXX	FRCC201100429	CIP-007-3	R1	FRCC_URE1 self-reported that it failed to perform the required testing when adding Cyber Assets, as required by CIP-007-3 R1. Specifically, a new server was added to FRCC_URE1's Electronic Security Perimeter (ESP) and appropriate testing controls were not performed. The server was accidentally installed and was removed six days later.	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 untested Cyber Asset was detected within six days. Second, the server was accidently installed and was never configured to communicate with any other device within the ESP or outside the ESP. Further, the untested Cyber Asset was removed from the ESP and configured as a non-Critical Cyber Asset workstation with no BPS control and monitoring function.	FRCC_URE1 certified that it completed its mitigation activities by promptly (6 days) removing the accidently-installed server.

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 2 (FRCC_URE2)	NCRXXXXX	FRCC2011007239	CIP-002-1	R2	During a Compliance Spot Check, FRCC discovered that FRCC_URE2 failed to properly apply its risk-based assessment methodology (RBAM) to develop a list of identified Critical Assets, as required by CIP-002-1 R2. Specifically, the list of Critical Assets provided by FRCC_URE2 did not correlate to the set of identification criteria included in its RBAM. FRCC_URE2's RBAM included explanation and development of a risk-based assessment approach and a resultant list of identification criteria for Critical Assets. From this list of identification criteria, the entity created a list of Critical Assets. The risk-based assessment approach developed within FRCC_URE2's RBAM included assessment of a "transmission substation" with greater than 1,200 MW of generation connected. However, when the final statement of the identification criteria was made in FRCC_URE2's RBAM, it incorrectly stated that a "generation site" greater than 1,200 MW should be considered a Critical Asset. As a result of this incorrect wording, a single generation site which contained greater than 1,200 MW was not listed as a Critical Asset. The final identification criteria in FRCC_URE2's RBAM that addressed a generation site greater than 1,200 MW appears to have been a wording error.	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 list of Critical Assets identified by FRCC_URE2 did correlate with all the correctly-stated criteria of FRCC_URE2's RBAM.	FRCC_URE2 certified that it completed its mitigation activities, which consisted of correcting the errors in the methodology to clearly articulate the generation impact that could occur related to a cyber event.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 2 (FRCC_URE2)	NCRXXXXX	FRCC2011007240	CIP-005-1	R1; R1.1; R1.5	During a Compliance Spot Check, FRCC discovered that FRCC_URE2 failed to identify and document the Electronic Security Perimeters (ESPs) and all access points to the perimeters, as required by CIP-005-1 R1. Specifically, FRCC_URE2 failed to identify certain modems connected to the communication server for communicating and data acquisition from the substations, as required by R1.1. Further, FRCC_URE2 failed to maintain recovery plans for electronic access control and monitoring devices, as required by R1.5. Additionally, FRCC_URE2 removed one set of intrusion detection system (IDS) devices and replaced it with another vendor product with same functionality but did not update the recovery plan to address the recovery of these Cyber Assets used in electronic access control and monitoring, as required by R1.5.	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 FRCC_URE2's access points that were not identified used serial-only communication. Even these access points were well-protected using appropriate communication controls and limited by configuration. Devices are only allowed to communicate to pre-configured remote terminal unit (RTU) and authentication between the access point device and the RTU is authenticated through a preconfigured code uniquely assigned to each RTU, and configured within the ESP access control device to allow communication to the designated RTU only.	FRCC_URE2 certified that it completed its mitigation activities by identifying and documenting the serial access points and updating the recovery plans to address the change in IDS devices.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007585	CIP-005-1	R2; R2.6	FRCC_URE3 self-reported that it failed to display a matching appropriate use banner and to document the content of the banner on all interactive attempts for all Electronic Security Perimeter (ESP) access point devices, as per its documented cyber security procedure. This condition existed for a period of approximately 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 FRCC_URE3 did display a banner but the banner text did not exactly match its own documented banner content. However, this was sufficient to notify and caution all those accessing the ESP without authorization.	FRCC_URE3 certified that it completed its mitigation activities by updating its risk-based assessment methodology (RBAM) and updating the text for the banners for all required ESP access point devices.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007807	CIP-006-2	R1; R1.6	During a Compliance Spot Check, FRCC discovered that FRCC_URE3 failed to ensure that continuous escorting and physical access logs were maintained for all visitors on one specific day and on one occasion, visitors' exit timings were not recorded.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). One instance of lack of recording the exit timings did not pose a significant security risk, as the records indicated that the visitor was from a trusted vendor and was continuously escorted.	FRCC_URE3 certified that it completed mitigation activities by updating its risk-based assessment methodology (RBAM), assessing all identified Physical Security Perimeters (PSPs), creating an awareness email for all appropriate staff and establishing a plan to review visitor logs on a weekly basis and follow up on any concerns with the appropriate party in a timely manner.
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007808	CIP-006-2	R2	During a Compliance Spot Check, FRCC discovered that FRCC_URE3 failed to identify six of its physical access control system (PACS) Cyber Assets and to afford them the protection required by CIP-006 R2.2. This condition existed for a period of approximately 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) as the subject PACS Cyber Assets were protected as per FRCC_URE3's own corporate security standards restricting any unauthorized access. Pursuant to FRCC_URE3's corporate security standards, only authorized persons are allowed within FRCC_URE3 facilities that host these systems. These facilities are considered secured facilities and access is monitored using video feeds. FRCC_URE3's PACS was secured within designated Physical Security Perimeters (PSPs) and all the remote equipment that was not within designated PSPs was on its own isolated network which could only be accessed after gaining control of the designated PSPs.	FRCC_URE3 certified that it completed mitigation activities by updating its PACS as a result of revision of its risk-based assessment methodology (RBAM) and updating the PACS inventory.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Florida Reliability Coordinating Council, Inc. (FRCC)	Unidentified Registered Entity 3 (FRCC_URE3)	NCRXXXXX	FRCC2011007806	CIP-007-1	R5	During a Compliance Spot Check, FRCC discovered that FRCC_URE3 failed to modify at least annually the passwords of multiple network users. This condition existed for a period of approximately two years.	This issue posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the network is always in a disabled state and procedural controls are used prior to any usage and authentication requires a security question response that is unique to each individual user. All of the network users at the time of the issue had completed a valid personnel risk assessment (PRA) and CIP training. Although FRCC_URE3 has a previous issue of noncompliance with this Standard, the instant remediated issue nonetheless does not represent recurring conduct by FRCC_URE3. The prior issue consists of a late-filed Technical Feasibility Exception regarding password complexity.	FRCC_URE3 certified that it completed mitigation activities by updating its network password and reviewing and updating the list of all network users.
Midwest Reliability Organization (MRO) and Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (URE1)	NCRXXXXX	MRO201100362 RFC2011001105	CIP-006-2	R1; R1.1	URE1 self-reported an issue with CIP-006-1 R1.1 for failing to submit a timely Technical Feasibility Exception (TFE) request in accordance with NERC procedures. The TFE request was submitted approximately 15 months beyond the required TFE submission window. URE1 could not provide a "six-wall" border for network cabling running between two Physical Security Perimeters (PSPs) because it would require URE1 to make the entire building a single PSP; and that solution would negatively impact operations without adding additional security.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. URE1 uses cabling to connect two PSPs in a single facility to the Electronic Security Perimeter (ESP). The cabling connecting the PSPs to the ESP is located above the ceiling within a non-public building protected by multiple physical access control layers.	URE1 submitted a TFE, which was approved.
Midwest Reliability Organization (MRO) and Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (URE1)	NCRXXXXX	MRO201100363 RFC2011001106	CIP-005-1	R2.6	URE1self-reported an issue with CIP-005-1 R2.6 for failing to submit timely Technical Feasibility Exception (TFE) requests in accordance with NERC procedures. The two TFE requests were submitted approximately 17 months beyond the required TFE submission window. URE1 could not afford the protective measures specified in CIP-005-1 R2.6 for Cyber Assets that authorize and/or log access to the Physical Security Perimeter (PSP), exclusive of hardware at the PSP. Specifically, it was not technically feasible for the electronic access control devices URE1 utilizes to authorize and/or log access to designated PSPs, to display appropriate use banners. Additionally, several Electronic Security Perimeter (ESP) access control and/or monitoring devices were also incapable of presenting the appropriate use banner for all methods of interactive access.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. The electronic access control devices are closed operating systems running on appliances; third-party software cannot be installed. Remote access to the electronic access control devices door controllers is protected by the use of a two-factor authentication system, including an intrusion detection system and multiple firewalls, and the electronic access control devices door controllers are located in secure areas within the PSP. Additionally, the ESP access control and/or monitoring devices are protected by PSPs and local access ports protected by tamper proof seals with access warnings, and global and local passwords at each access point.	URE1 submitted TFEs, which were approved.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 2 (MRO_URE1)	NCRXXXXX	MRO201100390	CIP-005-1	R1; R1.5	During a regularly scheduled Compliance Audit, MRO determined that MRO_URE1 failed to afford the measures afforded in CIP-007-3 R5 for Cyber Assets used in the control and monitoring of the Electronic Security Perimeter. Specifically, MRO_URE1 failed to implement and document technical and procedural controls as required by CIP-007-3 R5. For all affected firewalls, password complexity for local administrative accounts was subject only to procedural control, and not technical control. The devices were capable of enforcing password complexity via technical control.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. MRO_URE1's procedural controls required that passwords be a minimum of six characters, that each password consisted of a combination of alpha, numeric, and “special” characters, and that each password is changed at least annually, or more frequently based on risk. Additionally, MRO_URE1 provided evidence that all of the passwords met the procedural controls.	MRO_URE1 implemented technical controls. MRO has verified mitigation activities completion.
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 3 (MRO_URE2)	NCRXXXXX	MRO201100393	CIP-002-1	R1; R1.2.1; R1.2.3	During a Spot Check, conducted between June 16, 2011 through June 28, 2011, MRO determined that the MRO_URE2 failed to include adequate evaluation criteria for the assessment of control centers and generation resources in its risk-based assessment methodology (RBAM). Specifically, MRO_URE2's RBAM did not represent a stand alone methodology for control centers and generation resources and failed to define the criteria and steps it follows to identify these Critical Assets. Instead, criticality of the assets were predetermined with conclusory justifications.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. MRO_URE2 considered its control center a Critical Asset and provided it the protections in the CIP Reliability Standards. The protections were in place for all the Critical Cyber Assets (CCAs) both before and after the criteria were revised. Although MRO_URE2 did not include adequate evaluation criteria for the assessment of control centers or generation resources, after revising the evaluation criteria for control centers and generation resources, the generation resources were still not considered critical, and therefore, should not have been treated as Critical Assets.	MRO_URE2 revised its RBAM to include adequate evaluation criteria for the assessment of control centers and generation resources, and was verified by MRO.

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	NPCC2011009036	CIP-003-2	R2; R2.3	During a NPCC CIP Compliance Audit, it was discovered that NPCC_URE1 had an issue with CIP-003-2 R2.3. NPCC determined that a letter from an executive manager of NPCC_URE1 and senior manager having full authority and responsibility for CIP-002 through CIP-009 compliance verified that she had delegated authority to two other executives. This delegation of authority was not documented within thirty calendar days, as required by CIP-003-2 R2.3. The letter is relied upon by multiple affiliated registered entities for compliance with CIP-003-2 R2.3, including NPCC_URE1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because this was a matter of late documentation covering a span of only four calendar days. Also, there was no gap in senior management leadership, and no actions were taken pursuant to the changed delegations during the four-day period before the documentation was updated.	NPCC_URE1 documented the delegation of authority for specific actions to named delegates. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008338	CIP-003-2	R2; R2.3	NPCC_URE2 self-reported to NPCC an issue with CIP-003-2 R2.3. During a NPCC CIP Compliance Audit of its affiliate, it was discovered that both companies had an issue with CIP-003-2 R2.3. NPCC determined that a letter from the affiliate's executive manager and senior manager having full authority and responsibility for CIP-002 through CIP-009 compliance verified that she had delegated authority to two other executives. This delegation of authority was not documented within thirty calendar days, as required by CIP-003-2 R2.3. The letter is relied upon by multiple affiliated registered entities for compliance with CIP-003-2 R2.3, including NPCC_URE2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because this was a matter of late documentation covering a span of only four calendar days. Also, there was no gap in senior management leadership, and no actions were taken pursuant to the changed delegations during the four-day period before the documentation was updated.	NPCC_URE2 documented the delegation of authority for specific actions to named delegates. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008442	CIP-003-2	R2; R2.3	NPCC_URE3 self-reported to NPCC an issue with CIP-003-2 R2.3. During a NPCC CIP Compliance Audit of its subsidiary, it was discovered that both companies had an issue with CIP-003-2 R2.3. NPCC determined that a letter from the subsidiary's executive manager and senior manager having full authority and responsibility for CIP-002 through CIP-009 compliance verified that she had delegated authority to two other executives. This delegation of authority was not documented within thirty days, as required by CIP-003-3 R2.3. The letter is relied upon by multiple affiliated registered entities for compliance with CIP-003-2 R2.3, including NPCC_URE3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because this was a matter of late documentation covering a span of only four calendar days. Also, there was no gap in senior management leadership, and no actions were taken pursuant to the changed delegations during the four-day period before the documentation was updated.	NPCC_URE3 documented the delegation of authority for specific actions to named delegates. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009038	CIP-006-1	R1; R1.1	During a NPCC CIP Compliance Audit, it was discovered that NPCC_URE1 had an issue with CIP-006-1 R1.1. NPCC determined that NPCC_URE1's Electronic Security Perimeter, which resides within a Physical Security Perimeter where a completely enclosed ("six-wall") border was compromised by the ability of a person to access those areas through a raised floor area that was approximately 18 inches high.	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 while there was a gap in the “six-wall" border (approximately 18 inches), the Physical Security Perimeter had multiple layers of security that would minimize unauthorized access into the secure area. To access the area where the gap was located, it would require: (1) permission to enter at the perimeter gate that completely surrounds the building and is monitored constantly by security personnel or a badge reader; (2) permission to enter the special use building through a badge reader; and (3) permission to enter the secure area through a badge reader that is restricted to personnel who work in that area. Additionally, NPCC_URE1 conducts video surveillance on the access points to the secure area.	NPCC_URE1 installed barriers in the raised floor thereby eliminating the gap under the raised floor between two secure Physical Security Perimeter areas. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC2011009037	CIP-005-1	R2; R2.3	During a NPCC CIP Compliance Audit, it was discovered that NPCC_URE1 had an issue with CIP-005-1 R2.3. NPCC determined that NPCC_URE1's procedure for securing dial-up access to the Electronic Security Perimeters (ESPs) was created approximately three years after NPCC_URE1 was required to comply with the Standard. NPCC_URE1 could not demonstrate that there was a procedure in effect prior to that time. This procedure is relied upon by multiple affiliated registered entities for compliance with CIP-005-3 R2.3, including NPCC_URE1.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE1 provided evidence that demonstrated its commitment to securing its dial-up access points. First, dial-up access into the ESP is controlled by a system which utilizes multiple authentication controls including usernames, passwords, and other user authentication functions. Second, NPCC_URE1 does not allow dial-up access to its Energy Management System ESPs. Third, a presentation outlines how to secure the devices which are used to secure dial-up access. This presentation is given to the technicians responsible for installing the devices.	NPCC_URE1 created a procedure for securing dial-up access to the ESPs. The mitigation activity was verified complete by NPCC.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC2011008339	CIP-005-1	R2; R2.3	NPCC_URE2 self-reported to NPCC an issue with CIP-005-1 R2.3. During a NPCC CIP Compliance Audit of its affiliate, it was discovered that both companies had an issue with CIP-005-1 R2.3. NPCC determined that NPCC_URE2's parent company had a corporate procedure for securing dial-up access to the Electronic Security Perimeters (ESPs) which was created approximately three years after NPCC_URE2 was required to comply with the Standard. NPCC_URE2 could not demonstrate that there was a procedure in effect prior to that time. This procedure is relied upon by multiple affiliated registered entities for compliance with CIP-005-3 R2.3, including NPCC_URE2.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 provided evidence that demonstrated its commitment to securing its dial-up access points. First, dial-up access into the ESP is controlled by a system which utilizes multiple authentication controls including usernames, passwords, and other user authentication functions. Second, NPCC_URE2 does not allow dial-up access to its Energy Management System ESPs. Third, a presentation outlines how to secure the devices which are used to secure dial-up access. This presentation is given to the technicians responsible for installing the devices. Although NPCC_URE2 has violated this Standard previously, the instant remediated issue nonetheless does not represent recurring corporate conduct. The prior violation involved incomplete documentation of ports and services for Critical Cyber Assets.	NPCC_URE2 created a procedure for securing dial-up access to the ESPs. The mitigation activity was verified complete by NPCC.
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 3 (NPCC_URE3)	NCRXXXXX	NPCC2011008446	CIP-005-1	R2; R2.3	NPCC_URE3 self-reported to NPCC an issue with CIP-005-1 R2.3. During a NPCC CIP Compliance Audit of its subsidiary, it was discovered that both companies had an issue with CIP-005-1 R2.3. NPCC determined that NPCC_URE3's corporate procedure for securing dial-up access to the Electronic Security Perimeters (ESPs) was created approximately three years after NPCC_URE3 was required to comply with the Standard. NPCC_URE3 could not demonstrate that there was a procedure in effect prior to that time. This procedure is relied upon by multiple affiliated registered entities for compliance with CIP-005-3 R2.3, including NPCC_URE3.	This issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE3 provided evidence that demonstrated its commitment to securing its dial-up access points. First, dial-up access into the ESP is controlled by a system which utilizes multiple authentication controls including usernames, passwords, and other user authentication functions. Second, NPCC_URE3 does not allow dial-up access to its Energy Management System ESPs. Third, a presentation outlines how to secure the devices which are used to secure dial-up access. This presentation is given to the technicians responsible for installing the devices.	NPCC_URE3 created a procedure for securing dial-up access to the ESPs. The mitigation activity was verified complete by NPCC.
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100776	CIP-005-3	R4	RFC_URE1 self-reported an issue with CIP-005-3 R4 to Reliability*First*. In the Self-Report, the entity stated it failed to conduct its annual cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter (ESP) and of the Cyber Assets within the ESP. RFC_URE1 scheduled its annual cyber vulnerability assessment to occur concurrently with a planned major hardware and software upgrade of its Energy Management System/Supervisory Control and Data Acquisition (EMS/SCADA) and automatic generation control (AGC) systems; however, the hardware and software upgrade was delayed almost one month later. Due to the delay, RFC_URE1 conducted the cyber vulnerability assessment on its upgraded EMS/SCADA and AGC systems. Reliability*First* determined that RFC_URE1 had an issue with CIP-005-3 R4 when it did not perform an annual cyber vulnerability assessment of the electronic access points to the ESP and an annual cyber vulnerability assessment of all Cyber Assets within the ESP.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the risk was mitigated by the following factors. RFC_URE1 performed the cyber vulnerability assessment 21 days after the scheduled date. When RFC_URE1 later performed its cyber vulnerability assessment, RFC_URE1 assessed the upgraded EMS/SCADA and AGC. Therefore, RFC_URE1 assessed possible vulnerabilities and weaknesses of the upgraded EMS/SCADA and AGC systems rather than assessing the vulnerabilities and weaknesses for systems that RFC_URE1 was about to modify with major hardware and software upgrades.	RFC_URE1 submitted to Reliability*First* a Mitigation Plan to address the remediated issue of CIP-005-3 R4. In this Mitigation Plan, RFC_URE1 stated that it completed all mitigating actions necessary to address the remediated issue of CIP-005-3 R4. Specifically, RFC_URE1 completed the requisite cyber vulnerability assessment. Additionally, RFC_URE1 set up a notice in its compliance system that sends two employees a reminder to perform its annual cyber vulnerability assessment 60 days in advance of the due date. This notice will help ensure RFC_URE1 is not delinquent in performing its annual cyber vulnerability assessment.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100777	CIP-007-3	R8	RFC_URE1 self-reported an issue with CIP-007-3 R8 to Reliability*First* . In the Self-Report, RFC_URE1 stated it failed to conduct its annual cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter (ESP) and of the Cyber Assets within the ESP. RFC_URE1 scheduled its annual cyber vulnerability assessment to occur concurrently with a planned major hardware and software upgrade of its Energy Management System/Supervisory Control and Data Acquisition (EMS/SCADA) and automatic generation control (AGC) systems; however, the hardware and software upgrade was delayed almost one month later. Due to the delay, RFC_URE1 conducted the cyber vulnerability assessment on its upgraded EMS/SCADA and AGC systems. Reliability*First* determined that RFC_URE1 had an issue with CIP-007-3 R8 when it did not perform an annual cyber vulnerability assessment of the electronic access points to the ESP and an annual cyber vulnerability assessment of all Cyber Assets within the ESP.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because the risk was mitigated by the following factors. RFC_URE1 performed the cyber vulnerability assessment 21 days after the scheduled date. Additionally, when RFC_URE1 performed its cyber vulnerability assessment, RFC_URE1 assessed the upgraded EMS/SCADA and AGC. Therefore, RFC_URE1 assessed possible vulnerabilities and weaknesses of the upgraded EMS/SCADA and AGC systems rather than assessing the vulnerabilities and weaknesses for systems that RFC_URE1 was about to modify with major hardware and software upgrades.	RFC_URE1 submitted to Reliability*First* a Mitigation Plan to address the remediated issue of CIP-007-3 R8. In this Mitigation Plan, RFC_URE1 stated that it completed all mitigating actions necessary to address the remediated issue of CIP-005-3 R4. Specifically, RFC_URE1 completed the requisite cyber vulnerability assessment. Additionally, RFC_URE1 set up a notice in its compliance system that sends two employees a reminder to perform its annual cyber vulnerability assessment 60 days in advance of the due date. This notice will help ensure the entity is not delinquent in performing its annual cyber vulnerability assessment.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2012001313	CIP-007-3	R1	RFC_URE2 self-reported an issue with CIP-007-3 R1 to Reliability*First* , identifying an issue of CIP-007-3 R1. Pursuant to its procedure to test changes to Cyber Assets, RFC_URE2 documented test results for new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter (ESP) utilizing two forms, Form 1 and Form 2. Form 1 documented testing for new Cyber Assets within the ESP, and Form 2 documented testing for changes to Cyber Assets within the ESP. Form 2 also contained documentation of certain tests performed for new Cyber Assets within the ESP. When RFC_URE2 installed new operator workstations on four occasions for a two year period, RFC_URE2 completed Form 1, but not Form 2. RFC_URE2 failed to submit Form 2 because the individual responsible for doing so did not submit Form 2 until 30 to 120 days after the installation of the new operator workstations. Therefore, Reliability*First* determined that RFC_URE2 had an issue with the Standard for failing to complete the required documentation of testing performed on new Cyber Assets in the ESP.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system. RFC_URE2 completed Form 1 in each instance, which contains substantially the same information as Form 2. In addition, RFC_URE2 completed Form 2 for each of the devices when performing testing due to operating system security patches, within 30 to 120 days after the initial installation.	In order to mitigate the issue, RFC_URE2 replaced Form 1 and Form 2 with a single form and revised its procedures to include this single form. Reliability*First* verified that RFC_URE2 completed the mitigating activities.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100873	CIP-003-1	R6	RFC_URE3 self-reported that during an internal assessment of CIP compliance, it discovered that it failed to document its assessment and application of certain patches on five applications. Since RFC_URE3 failed to monitor these Cyber Assets pursuant to CIP-007-1, it also failed to comply with CIP-003-1 R6. ReliabilityFirst determined that RFC_URE3 had an issue with the Standard for failing to implement supporting configuration management activities. The duration of the issue spans versions 1 through 3 of the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The affected applications are considered non-critical Cyber Assets, and only one of the five affected applications had been issued a security patch by its original manufacturer over the duration of the issue. Although RFC_URE3 failed to document its assessment and application of certain patches on five applications, it assessed and applied patches for 97.8% of the applications within its Electronic Security Perimeter. Additionally, RFC_URE3 otherwise has an established change management program that includes associated procedures and supporting technology for implementation. Lastly, the affected Cyber Assets are protected by RFC_URE3's comprehensive "defense-in-depth" security strategy.	RFC_URE3 submitted to Reliability*First* its Mitigation Plan to address the issue of NERC Reliability Standard CIP-003-1 R6. In the Mitigation Plan, RFC_URE3 memorialized the actions it took to address the issue with NERC Reliability Standard CIP-003-1 R6 and committed to additional actions to prevent future risk to the BPS. RFC_URE3 documented the implementation of identified patches and is undertaking significant, multi-faceted efforts to develop and implement an improved patch management process, including revisions to associated, dependent processes, such as RFC_URE3's established change management program. RFC_URE3 completed the Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100874	CIP-006-1	R2	RFC_URE3 self-reported that it discovered an issue with NERC Reliability Standard CIP-006-1 R2. In response to its discovery of possible noncompliance with CIP-007-3 R3 and CIP-003-1 R6, RFC_URE3 reviewed the affected Cyber Assets to assess its compliance with CIP-006-1 R2. This assessment identified Cyber Assets used to authorize or log access to the Physical Security Perimeter that did not receive all applicable cyber security software patches. These Cyber Assets are desktop computers that were subject to a vendor maintenance contract. Although the desktop computers were patched according to the vendor's security software application, they were not patched relative to the installed operating systems and software applications. Since RFC_URE3 failed to consistently implement patches on these desktop computers, they were not afforded the protections of CIP-007-1 R3 and CIP-003-1 R6, as required by CIP-006-1 R2. The duration of the issue spanned versions 1 through 3c of the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The desktop computer Cyber Assets involved in this issue were properly patched six months before the Self-Report and had received some patches through the vendor's security-related software application up until that time. In addition, RFC_URE3 has an established change management program that includes associated procedures and supporting technology for implementation. Lastly, the affected Cyber Assets are protected by RFC_URE3's comprehensive "defense-in-depth" security strategy of the BPS.	RFC_URE3 submitted to Reliability*First* its Mitigation Plan to address the issue with NERC Reliability Standard CIP-006-1 R2. In this Mitigation Plan, RFC_URE3 memorialized the actions it took to address the issue with NERC Reliability Standard CIP-006-1 R2 and committed to additional actions to prevent future risk to the BPS. RFC_URE3 documented the implementation of identified patches and is undertaking significant, multi-faceted efforts to develop and implement an improved patch management process, including revisions to associated, dependent processes, such as RFC_URE3's established change management program. RFC_URE3 completed the Mitigation Plan.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100875	CIP-007-1	R3	RFC_URE3 self-reported that during an internal assessment of CIP compliance, it discovered an issue with NERC Reliability Standard CIP-007-1 R3. ReliabilityFirst determined that RFC_URE3 had an issue with NERC Reliability Standard CIP-007-1 R3 by failing to consistently implement and document its efforts related to the tracking, evaluating, testing, and installation of applicable security patches for certain applications that are considered non-critical Cyber Assets within the Electronic Security Perimeter (ESP). The duration of the issue spans versions 1 through 3 of the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). All affected applications are considered non-critical Cyber Assets, and only one of the five affected applications had been issued a security patch by its original manufacturer over the duration of the issue. Although RFC_URE3 failed to document its assessment and application of certain patches on five applications, it assessed and applied patches for 97.8% of the applications within its ESP. Additionally, RFC_URE3 otherwise has an established change management program that includes associated procedures and supporting technology for implementation. Lastly, the affected Cyber Assets are protected by RFC_URE3's comprehensive "defense-in-depth" security strategy.	RFC_URE3 submitted to Reliability*First* its Mitigation Plan to address the issue with CIP-007-3 R3. In this Mitigation Plan, RFC_URE3 memorialized the actions it took to address the issue with NERC Reliability Standard CIP-007-3 R3 and committed to additional actions to prevent future risk to the BPS. RFC_URE3 documented the implementation of identified patches and is undertaking significant, multi-faceted efforts to develop and implement an improved patch management process, including revisions to associated, dependent processes, such as RFC_URE3's established change management program. RFC_URE3 completed this Mitigation Plan.
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100949	CIP-005-1	R1	RFC_URE3 self-reported an issue with CIP-005-1 R1. RFC_URE3 discovered certain non-critical software components installed on Cyber Assets within an Electronic Security Perimeter (ESP) had not been identified in RFC_URE3's documentation of Cyber Assets in the ESP as required by NERC Reliability Standards CIP-005-1 R1.4 and R1.6. More specifically, RFC_URE3 failed to categorize certain software components as non-critical Cyber Assets and, as a result, did not include those software components in its CIP compliance efforts aimed at identification and documentation of Cyber Assets in the ESP. As a result of RFC_URE3's failure to identify all non-critical Cyber Assets within a defined ESP, it also failed to comply with NERC Reliability Standard CIP-005-1 R5. The duration of the issue spans versions 1 through 3a of the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Cyber Assets on which the software components were installed were identified as non-critical Cyber Assets and were protected by the ESP itself and RFC_URE3's established "defense-in-depth" security strategy. Furthermore, the software components were maintained in accordance with RFC_URE3's corporate processes, policies, and procedures, including its change management process, which afforded additional protection such as: (a) a requirement for a change ticket whenever a production change or modification is implemented; (b) a requirement that change tickets must include a test plan, test results, any variances or exceptions, and approvals by affected internal stakeholders to execute the change (including Real-Time Operations, where applicable); (c) a requirement that both internal and external notifications of planned modifications be made to affected stakeholders; (d) corporate-level archival of change tickets and RFC_URE3 source code; and (e) corporate-level version-control of RFC_URE3 source code.	RFC_URE3 submitted to Reliability*First* its Mitigation Plan to address the issue with NERC Reliability Standard CIP-005-1 R1. In this Mitigation Plan, RFC_URE3 memorialized the actions it took to address the issue with NERC Reliability Standard CIP-005-1 R1 and committed to additional actions to prevent future risk to the BPS. RFC_URE3 finalized its list of installed, non-critical software components and documented a formal process for control and maintenance of these software components. RFC_URE3 also relocated applications for which ESP protection is not necessary, which facilitates compliance by appropriately concentrating protection and compliance efforts. RFC_URE3 completed the Mitigation Plan.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Reliability*First* Corporation (Reliability*First)*	Unidentified Registered Entity 3 (RFC_URE3)	NCRXXXXX	RFC201100950	CIP-005-1	R5	RFC_URE3 self-reported an issue with CIP-005-1 R5. RFC_URE3 reported that it discovered certain non-critical software components installed on Cyber Assets within an Electronic Security Perimeter (ESP) had not been identified in RFC_URE3's documentation of Cyber Assets in the ESP as required by NERC Reliability Standards CIP-005-1 R1.4 and R1.6. More specifically, RFC_URE3 failed to categorize certain software components as non-critical Cyber Assets and, as a result, did not include those software components in its CIP compliance efforts aimed at identification and documentation of Cyber Assets in the ESP. As a result of RFC_URE3's failure to identify all non-critical Cyber Assets within a defined ESP, it also failed to comply with NERC Reliability Standard CIP-005-1 R5. The duration of the issue spans versions 1 through 3a of the Standard.	Reliability*First* determined that this issue posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The Cyber Assets on which the software components were installed were identified as non-critical Cyber Assets and were protected by the ESP itself and RFC_URE3's established "defense-in-depth" security strategy. Furthermore, the software components were maintained in accordance with RFC_URE3's corporate processes, policies, and procedures, including its change management process, which afforded additional protection such as: (a) a requirement for a change ticket whenever a production change or modification is implemented; (b) a requirement that change tickets must include a test plan, test results, any variances or exceptions, and approvals by affected internal stakeholders to execute the change (including Real-Time Operations, where applicable); (c) a requirement that both internal and external notifications of planned modifications be made to affected stakeholders; (d) corporate-level archival of change tickets and RFC_URE3 source code; and (e) corporate-level version-control of RFC_URE3 source code.	RFC_URE3 submitted to Reliability*First* its Mitigation Plan to address the issue with NERC Reliability Standard CIP-005-1 R5. In this Mitigation Plan, RFC_URE3 memorialized the actions it took to address the issue with NERC Reliability Standard CIP-005-1 R5 and committed to additional actions to prevent future risk to the BPS. RFC_URE3 finalized its list of installed, non-critical software components and documented a formal process for control and maintenance of these software components. RFC_URE3 also relocated applications for which ESP protection is not necessary, which facilitates compliance by appropriately concentrating protection and compliance efforts. RFC_URE3 completed the Mitigation Plan.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC2012009232	CIP-003-2	R2	During an internal review of the CIP Standards, WECC_URE1 self-certified that it did not own any Critical Assets (CAs) or Critical Cyber Assets (CCAs). In the past, WECC_URE1 was not required to be compliant with CIP-003 through CIP-009 because WECC_URE1 did not have CAs or CCAs. This was accurate until April 1, 2010 when CIP-003-2 became enforceable for WECC_URE1 due to changes to Section 4.2.3 of CIP-003-2. The change required CIP-003-2 R2 to apply to all Responsible Entities, including Responsible Entities that have no CCAs. WECC_URE1 failed to notice this change in the Standard and as a result failed to assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002-2 through CIP-009-2, as required by CIP-003-2 R2.	Although WECC_URE1 failed to assign a senior manager as required by CIP-003-2 R2, WECC determined that the issue posed a minimal risk to the reliability of the bulk power system because: 1. The entity has no CAs or CCAs. 2. The entity does not own or operate any facilities that would meet any of the Critical Asset Identification Criteria.	WECC_URE1 assigned a senior manager with the overall responsibility and authority for leading and managing the implementation of and adherence to CIP-002 through CIP-009.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC2012009097	CIP-007-3	R9	WECC_URE2 submitted a Self-Report stating that it had failed to document changes made to CIP-007-3 R5 procedure/policy within 30 days, pursuant to CIP-007-3 R9. Specifically, WECC_URE2 reported that the department responsible for the support of the network devices in the Emergency Management System (EMS) environment created a process document to capture the procedures and policies for "account management" as specified by R5. It was discovered that while the document does address R5.3, the information listed related to the authentication password controls for access to Critical Cyber Assets (CCAs) was out of date and had not been updated when a new authentication solution was implemented a year earlier. The change to the CIP-007-3 R5 procedure/policy occurred a year earlier, WECC_URE2 did not detect the issue and revise documentation until a year later, therefore, WECC_URE2 failed to document revised procedure within 30 days as required by CIP-007-3 R9.	WECC determined this issue posed minimal risk to the reliability of the bulk power system (BPS) because WECC_URE2 implemented procedures consistent with CIP-007-3. As compensating measures, WECC_URE2 stated that new password controls are stricter, e.g. the new systems require a minimum password length of 12 characters. WECC_URE2 states that all password controls required by the CIP-007 R5 standard were implemented. WECC, therefore, determined the risk posed by this issue was minimal.	WECC_URE2 updated CIP-007-3 R5 documentation to reflect revised process.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 3 (WECC_URE3)	NCRXXXXX	WECC2012009688	CIP-002-3	R4	During an Audit, WECC found that WECC_URE3 was noncompliant with CIP-002-3 R4 because it did not maintain a signed and dated list of its Critical Cyber Assets (CCAs). The entity does not have any CCAs, thus making this list a null set.	WECC determined this issue posed a minimal risk to the reliability of the bulk power system because the entity did not have any CCAs in accordance with its risk-based assessment methodology (RBAM). Although the entity did not maintain a signed and dated list of its CCAs, it does have in place a RBAM and a list of Critical Assets (CAs). Both of these documents are signed and dated by the entity's manager of a delegate thereof. Additionally, WECC verified that the entity mitigated the violation when it created a list of CCAs and had it signed by a senior manager.	The entity mitigated the violation when it created a list of CCAs and had it signed by a senior manager.

City of Palo Alto

Southwest Transmission Cooperative, Inc.

Region	Name of Entity	NCR	Issue Tracking #	Standard	Req.	Description of Remediated Issue	Description of the Risk Assessment	Description and Status of Mitigation Activity
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 4 (WECC_URE4)	NCRXXXXX	WECC201102826	CIP-007-1	R6	WECC_URE4 performed an in-depth inventory of the Cyber Assets contained within the Electronic Security Perimeters (ESPs) for its substations. As a result of that inventory, WECC_URE4 discovered Cyber Assets that require a Technical Feasibility Exception (TFE) for CIP-007-1 Requirement 6. In total, 138 Critical Cyber Assets and 18 non-critical Cyber Assets located within 12 ESPs lacked the capability to implement automated tools or organizational process controls to monitor system events that are related to cyber security. WECC_URE4 self-reported that it had an issue with the CIP Standards arising from the entity's failure to timely submit TFE Requests in accordance with NERC procedures. The Self-Report referenced all identified TFEs that should have been filed as of that point. Specifically, WECC_URE4 submitted 37 late TFE Requests for CIP-007-1 R6.	WECC reviewed and accepted the TFE and determined it is technically infeasible for the entity to comply with the Standard for the devices associated with the TFE Identification number. The compensating measures, described below, were in place prior to the due date on which all such TFE requests were to originally be submitted to WECC. The entity had an implemented intrusion detection system (IDS) which monitors all network traffic and sends automated alerts upon detecting suspicious traffic. All devices in scope are located in Physical Security Perimeters and ESPs and thus afforded the protections of CIP-005 and CIP-006. Additionally, all individuals with access to the devices have a valid Personnel Risk Assessment and training. For these reasons, WECC determined that this issue posed minimal risk to the reliability of the bulk power system.	Entity filed the TFEs, WECC approved the Part A and Part B TFE.
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 5 (WECC_URE5)	NCRXXXXX	WECC2011008701	CIP-004-3	R4	WECC_URE5 self-reported an issue of CIP-004-3 R4. A WECC subject matter expert (SME) contacted WECC_URE5 to discuss its Self Report. According to the WECC SME, during the conversation, WECC_URE5 stated that it failed to update its access list and revoke access for two former employees within seven days of their leaving WECC_URE5 employment. The first employee left on August 5, 2011, and that employee's access should have been revoked by August 12, 2011 but was not revoked until August 30, 2011. The second employee left WECC_URE5 on August 12, 2011 and that employee's access should have been revoked on August 19, 2011 but was not revoked until September 13, 2011. According to the WECC SME, WECC_URE5 stated that these employees' manager failed to notify WECC_URE5's compliance department that the employees had left WECC_URE5 employment and, as a result, their access was not timely revoked and WECC_URE5's access list was not updated.	The employees in scope had physical access to a Physical Security Perimeter (PSP) that contains Critical Cyber Assets (CCAs), but did not have electronic access to the CCAs. The employees had personal risk assessments (PRA) and training prior to getting physical access the CCAs. The CCAs in scope are located in a locked cabinet that had monitoring and logging measures to detect any unauthorized activity. For these reasons, WECC determined that this issue posed a minimal risk to the bulk power system.	WECC_URE5 revoked the access of the individuals involved in the violation and distributed an email outlining WECC_URE5's process for revoking employee's access to CCAs.

Document Accession #: 20120430-5663 Filed Date: 04/30/2012

Document Content(s)