Federal Energy Regulatory Commission
Washington, D.C. 20426

August 30, 2021

Re: Thirty First 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 2020, in which you requested information pursuant to the Freedom of Information Act (FOIA),[1] and the Federal Energy Regulatory Commission's (Commission) FOIA regulations, 18 C.F.R. § 388.108 (2019).

By letter dated August 10, 2021, the submitter and the concerned Unidentified Registered Entity (URE) were informed that a copy of the public version of the Notice of Penalty associated with Docket No. NP12-12, along with the name of a relevant URE inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the document is enclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or to discuss any aspect of your request, you may contact Assistant United States Attorney April D. Seabrook by email at april.seabrook@usdoj.gov, by phone at (202) 252-2525, or

[1] 5 U.S.C. § 552 (2018).

[2] This docket involved multiple UREs and notification of the FOIA request as well as the Notice of Intent to Release were only sent to the URE for whom FERC determined that disclosure of its identities was appropriate.

by mail at United States Attorney's Office – Civil Division, U.S. Department of Justice, 555 Fourth Street, N.W., Washington, DC 20530.

Sincerely,

BENJAMIN WILLIAMS
Digitally signed by BENJAMIN WILLIAMS
Date: 2021.08.27 12:27:13 -04'00'

Benjamin Williams
Deputy Director
Office of External Affairs

Enclosure

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

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

Document Accession #: 20120215-5145 Filed Date: 02/15/2012

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

February 15, 2012

NP12-12
NextEra Energy Resources, LLC
see .pdf page 34

VIA ELECTRONIC FILING

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

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. NP12-12-000

On January 31, 2012, the North American Electric Reliability Corporation (NERC) submitted a Spreadsheet Notice of Penalty regarding violations for 18 Registered Entities. By this filing, NERC submits an errata to correct the record with the following information.

NERC corrects two typographical errors that were made to the public version of the spreadsheet. Accordingly, NERC submits a replacement version and provides the public versions in their entirety for convenience.

Accordingly, NERC respectfully requests that the Commission accept this supplemental filing and issue an order accepting the Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Rebecca J. Michael
Rebecca J. Michael
Attorney for North American Electric Reliability Corporation

Enclosures: Corrected Spreadsheets and Public Version of Filing

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

Document Accession #: 20120215-5145 Filed Date: 02/15/2012

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

January 31, 2012

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. NP12-__-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 18 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 51 violations[5] of 18 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.

NERC notes that violation FRCC201100422 was originally processed as an FFT in the November 30, 2011 informational filing. Based upon additional information received regarding the underlying violation, and in consideration that there was manual local load shedding albeit controlled and limited to prevent further issues, NERC has determined that the violation is more appropriately processed as an NOP. Accordingly, it is included in the instant filing.

As discussed below, this Spreadsheet NOP resolves 51 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 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.

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 violations in the Spreadsheet were approved by NERC Enforcement staff under delegated authority from the NERC Board of Trustees Compliance Committee. Such considerations include the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, the NERC Enforcement staff'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 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.	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

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
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

Spreadsheet Notice of Penalty
(Included in a Separate Document)

Document Accession #: 20120215-5145 Filed Date: 02/15/2012

NERC

Attachment b

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR JANUARY 2012 SPREADSHEET NOP INFORMATIONAL FILING

FOR FRCC:

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

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

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

FOR MRO:

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

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

FOR RFC:

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

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

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

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

FOR 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

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.

- 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 Violation Risk Factor (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. The VRFs for CIP-004-2 R2 were not changed when CIP-004-2 went into effect on April 1, 2010. The VRFs for CIP-004-3 R2 were not changed when CIP-004-3 went into effect on October 1, 2010.

- 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. The VRFs for CIP-004-3 R3 were not changed when CIP-004-3 went into effect on October 1, 2010.

- 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-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. The VRFs for CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8 and R1.9 were not changed when CIP-006-2 went into effect on April 1, 2010. The VRFs for CIP-006-3 R1, R1.1, R1.2, R1.3, R1.4, R1.5, R1.6, R1.7, R1.8 and R1.9 were not changed when CIP-004-3 went into effect on October 1, 2010. Two new sub-requirements were added to Version 3 of the standard; CIP-006-3 R1.6.1 and R1.6.2 each have Medium VRFs.

- 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 R4, R4.1 and R4.2 each have a Medium VRF. When NERC filed VRFs it originally assigned CIP-007-1 R4, R4.1 and R4.2 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 2, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-007-1 R4, R4.1 and R4.2 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.

- When NERC filed VRFs it originally assigned COM-002-2 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 Lower VRF for COM-002-2 R1 was in effect from June 18, 2007 until August 9, 2007 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 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. NP12-___-000

NOTICE OF FILING
January 31, 2012

Take notice that on January 31, 2012, the North American Electric Reliability Corporation (NERC) filed a Spreadsheet Notice of Penalty regarding eighteen (18) Registered Entities in five (5) 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

January 31, 2012 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	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Florida Reliability Coordinating Council, Inc. (FRCC)	JEA	NCR00040	FRCC201100422	Settlement Agreement	On March 8, 2011, JEA submitted a Self-Report to FRCC that as a Transmission Operator, it was in violation of TOP-004-2 R1 because during a one-day event on January 13, 2011, a failed static wire resulted in the outage of two 138 kV transmission lines. These outages led to what appeared to be MVA limit conditions on a 230/138 kV autotransformer. Although the System Operating Limit (SOL) was exceeded because the autotransformer had been rated conservatively, there was no Interconnection Reliability Operating Limit (IROL) exceedance. The system operator initiated a load shed of the entity's local load (approximately 135 MW) for approximately one hour to resolve what appeared to be a transformer overload. There was no instability, uncontrolled separation, or cascading outages that did occur or would have resulted from the loss of the transformer. Tests performed after the event indicated that the autotransformer in question had been rated conservatively and was not overloaded, had not been damaged and was not at risk of failure. Moreover, because the entity had an existing rating methodology under FAC-008 and followed it pursuant to FAC-009, FRCC concluded that there were no other related violations.	TOP-004-2	R1	High	High	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 although the outage of the two 138 kV circuits, led to indicated MVA limit conditions on the Hartley 230/138 kV autotransformer, even if the transformer had tripped, the result would have been limited to loss of local entity internal load. In fact, the manual load shed performed to correct the exceedance affected only local load. There would not be any instability, uncontrolled separation, or cascading outages resulting from the loss of the Hartley 230/138 kV autotransformer because the transformer would have only affected loss of local entity internal load. Also, although there appeared to be an overload on the autotransformer, due primarily to cold weather, the autotransformer was never actually overloaded because it had been rated conservatively. This was confirmed by subsequent review of industry standards, dissolved gas analysis and electrical testing of the autotransformer which showed the transformer was actually under rated.	1/13/2011 (start date of event)	1/13/2011 (end date of event)
Reliability*First* Corporation (Reliability*First*)	Allegheny Energy Supply Company, L.L.C. [GO, GOP] (AE Supply)	NCR02600	RFC2011001050	Settlement Agreement	On June 16, 2011, AE Supply submitted a Self-Report to Reliability*First* reporting a violation of VAR-002-1.1a. AE Supply initially self-reported six occasions on which it failed to notify its Transmission Operator (TOP) of an unexpected change in the status of a generator reactive power resource, however, after further investigation, AE Supply discovered three additional occasions when it did not notify its TOP of an unexpected change in the status of a generator reactive power resource. The changes in status involved placing the Automatic Voltage Regulator (AVR) into manual mode for each occasion. For six of the nine occasions, AE Supply exceeded the 30-minute notification requirement by a range of six minutes to 104 hours and 52 minutes. The remaining three occasions involved instances in which the change in status lasted fewer than 30 minutes and AE Supply did not inform its TOP of the change. Reliability*First* determined that AE Supply, as a Generator Operator (GOP), failed to notify its TOP within 30 minutes of a change in the status of a generator reactive power resource on nine separate occasions.	VAR-002-1.1a	R3	Medium	High	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because generators provide reactive and voltage control necessary to ensure voltage levels, reactive flows, and reactive resources are maintained within applicable Facility Ratings to protect equipment and the reliable operation of the BPS. This violation did not pose a serious or substantial risk to the reliability of the BPS because during each of the nine occasions, AE Supply manually controlled voltage, and maintained the generator voltage or reactive power output as directed by the TOP.	5/27/2010 (Date of the first occasion on which AE Supply exceeded the 30-minute notification requirement contained within the Standard)	6/6/2011 (Date of the last occasion on which AE Supply exceeded the 30-minute notification requirement contained within the Standard)
Reliability*First* Corporation (Reliability*First)*	Big Sandy Peaker Plant, LLC (BSPP)	NCR00690	RFC201100944	Settlement Agreement	On May 26, 2011, BSPP, as a Generator Owner (GO), self-reported noncompliance with FAC-008-1 R1 prior to a scheduled compliance audit. In May, 2007, BSPP identified its gas turbine generators as the most limiting equipment, but did not conduct a review of the associated electrical systems. On April 22, 2008, BSPP documented its Facility Ratings Methodology; however, Reliability*First* determined in a July 2011 Compliance Audit that this 2008 Methodology did not address terminal equipment, as required by the Standard. As a result, Reliability*First* determined that from June 18, 2007, when BSPP was required to comply with the Standard, through April 22, 2008, BSPP did not have a documented Methodology that included terminal equipment pursuant to R1 of the Standard. During the July 2011 Compliance Audit, Reliability*First* also determined that BSPP's most recent April 19, 2011 Methodology document did properly address terminal equipment. Thus, from April 22, 2008, when BSPP first documented its Methodology, through April 19, 2011, the date the latest Methodology came into effect, BSPP failed to have a Methodology that included terminal equipment, as required by R1.2.1 of the Standard.	FAC-008-1	R1	Medium	Severe	This violation posed a minimal risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by two factors. First, although prior to April 22, 2008, BSPP did not have a documented Methodology, BSPP had identified its gas turbine generators as the most limiting piece of equipment in its facility. Since documenting its Methodology on April 22, 2008 and revising it on April 19, 2011, BSPP confirmed that it correctly listed the gas turbine generators as the most limiting piece of equipment. Second, the rating for the gas turbine generators remains unchanged from the one produced by the 2008 Methodology.	6/18/2007 (when BSPP became subject to compliance with FAC-008-1 R1)	4/19/2011 (when BSPP revised its Methodology to include terminal equipment)

Attachment A-1

January 31, 2012 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	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Reliability*First* Corporation (Reliability*First)*	Big Sandy Peaker Plant, LLC (BSPP)	NCR00690	RFC201100945	Settlement Agreement	On May 26, 2011, BSPP, as a Generator Owner (GO), self-reported noncompliance with FAC-009-1 R1 prior to a scheduled compliance audit. Prior to April 22, 2008, BSPP did not have a documented Methodology and therefore could not have Facility Ratings that were consistent with its Methodology, as required by FAC-009-1, R1. Additionally, during the compliance audit, ReliabilityFirst determined that BSPP's Methodology, dated April 22, 2008, was not sufficient to demonstrate compliance with FAC-009-1, RI. Specifically, ReliabilityFirst was unable to determine the limiting element of the facility according to the scope of equipment listed under FAC-008, R 1.2.1 due to different units of measure (MVA/Amps). ReliabilityFirst also could not locate ratings for relay Protection System devices and series and shunt compensation devices based on the April 22. 2008 Methodology. From June 18, 2007, when BSPP was required to comply with the Standard, through April 22, 2008, BSPP did not have an adequately documented Methodology and therefore could not have Facility Ratings that are consistent with its Methodology, as required by the Standard. From April 22, 2008, when BSPP first documented its methodology, through April 19, 2011, BSPP failed to establish Facility Ratings that were consistent with its Methodology, as required by the Standard.	FAC-009-1	R1	Medium	Severe	This violation posed a minimal risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by two factors. First, although prior to April 22, 2008, BSPP did not have a documented Methodology, BSPP had identified its gas turbine generators as the most limiting piece of equipment in its facility. Since documenting its Methodology on April 22, 2008 and revising it on April 19, 2011, BSPP confirmed that it correctly listed the gas turbine generators as the most limiting piece of equipment. Second, the rating for the gas turbine generators remains unchanged from the one produced by the 2008 Methodology.	6/18/2007 (when BSPP became subject to compliance with FAC-009-1 R1)	4/19/2011 (when BSPP utilized its revised Methodology to develop Facility Ratings pursuant to FAC-009-1 R1)
Reliability*First* Corporation (Reliability*First)*	Big Sandy Peaker Plant, LLC (BSPP)	NCR00690	RFC201100946	Settlement Agreement	On May 26, 2011, BSPP, as a Generator Owner (GO), self-reported noncompliance with PRC-005-1 R1 prior to a scheduled compliance audit. From June 18, 2007, when BSPP was required to comply with the Standard, through April 22, 2008, BSPP did not have a documented Protection System maintenance and testing program (Program), as required by the Standard. Reliability*First* further concluded during a July 2011 compliance audit that BSPP's April 22, 2008 documented Program did not satisfy the requirements of the Standard. Specifically, Reliability*First* determined that the April 22, 2008 Program "only provides the compliance framework for BSPP and basically repeats the standard." On May 6, 2011, BSPP revised its Program to include a basis for all Protection System devices. Upon further review, ReliabilityFirst determined the basis for BSPP's voltage and current sensing devices which BSPP based on a draft version of Reliability Standard PRC-005-2 was not an acceptable basis as the draft standard has not been approved. On July 14, 2011, BSPP revised its Program to include an acceptable basis for maintenance and testing of voltage and current sensing devices. Thus, from June 18, 2007 through May 6, 2011, BSPP failed to adequately document its Program, as required by the Standard. From May 6, 2011, through July 18, 2011, BSPP did not have an acceptable basis in its Program for maintenance and testing of voltage and current sensing devices. BSPP's Program includes a total of 163 Protection System devices, consisting of 44 relays, 52 CTs/PTs, 4 Battery Banks and 63 DC Control Circuits.	PRC-005-1	R1	High	Severe	This violation posed a moderate risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following: BSPP (1) performed routine maintenance on relays and batteries during the duration of the alleged violation, (2) conducted maintenance and testing on its Protection System relays on a four year interval, (3) conducted maintenance and testing on its batteries on annual and quarterly intervals, and (4) reviewed all plant events and has had no Protection System misoperations.	6/18/2007 (when BSPP became subject to compliance with PRC-005-1 R1)	7/18/2011 (when BSPP included an acceptable basis for maintenance and testing of voltage and current sensing devices in its Program)
Reliability*First* Corporation (Reliability*First)*	Big Sandy Peaker Plant, LLC (BSPP)	NCR00690	RFC201100947	Settlement Agreement	On May 26, 2011, BSPP, as a Generator Owner (GO), self-reported noncompliance with PRC-005-1 R.2.1 prior to a scheduled compliance audit. Reliability*First* determined that BSPP could not provide evidence that it maintained its DC Control Circuits within defined intervals, in violation of this Standard. The DC Control Circuits were included in the May 6, 2011 Maintenance and Testing program.	PRC-005-1	R2.1	High	Severe	This violation posed a moderate risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by two factors. First, as part of the start-up process, each generating unit has various system health checks, including checks of DC Control Circuits. For example, a health monitoring circuit which monitors the lockout relay trip circuit is in effect on approximately 50% of BSPP's Protection System DC Control Circuits. BSPP used successful equipment starts to monitor the proper functioning of the DC Control Circuits. Second, BSPP reviewed all plant events and has had no Protection System misoperations.	6/18/2007 (when BSPP became subject to compliance with PRC-005-1 R2)	9/26/2011 (when BSPP completed its maintenance and testing)

Attachment A-1

January 31, 2012 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	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Reliability*First* Corporation (Reliability*First*)	Buckeye Power, Inc. (Buckeye Power)	NCR00700	RFC201000653	Settlement Agreement	During a Compliance Audit, conducted from September 13, 2010 through September 28, 2010, Reliability*First* discovered a violation of FAC-008-1 R1.2.1. Buckeye Power, as a Generator Owner, failed to include the ratings methodology for its transmission conductors, relay protective devices and terminal equipment in earlier versions of its Facility Ratings Methodology. Specifically, Reliability*First* reviewed Revisions 0 through 3 of the Facility Ratings Methodology utilized by Buckeye Power. Revision 0 is dated September 13, 2007; Revision 1 is dated June 15, 2009; Revision 2 is dated August 6, 2009; and Revision 3 is dated December 18, 2009. Reliability*First* determined that Revisions 0, 1 and 2 of Buckeye Power's Facility Ratings Methodology did not include transmission conductors, relay protective devices and terminal equipment. The current version of Buckeye Power's Facility Ratings Methodology, Revision 3, effective on December 18, 2009, included transmission conductors, relay protective devices and terminal equipment. Reliability*First* determined that Buckeye Power violated the Standard by failing to include transmission conductors, relay protective devices and terminal equipment in the scope of equipment addressed within the Facility Ratings Methodology in prior versions of the document.	FAC-008-1	R1; R1.2.1	Medium	Severe	In light of the nature of the violation, offset by the mitigating factors, Reliability*First* determined that the violation posed a minimal, not serious or substantial, risk to the reliability of the bulk power system (BPS). The risk to the reliability of the BPS was mitigated because Buckeye Power's Facility Ratings were based upon its most limiting element being, by design, its generators. In Revision 0, Buckeye Power included generators in the scope of equipment addressed in its Facility Ratings Methodology. As a result, generators are, and have always been, the most limiting element of Buckeye Power's facility. Buckeye Power's subsequent revisions to its Facility Ratings Methodology did not change the Facility Ratings. Buckeye Power designed its generating facilities such that the transmission elements within its system never limit a generating unit's output. Thus, Buckeye Power's identification of the most limiting element was always correct, and thereby mitigated the risk to the BPS posed by its insufficiently detailed Facility Ratings Methodology.	6/18/2007 (When the Standard became mandatory and enforceable)	12/18/2009 (When Buckeye Power updated its Facility Ratings Methodology to include transmission conductors, relay protective devices and terminal equipment)
Reliability*First* Corporation (Reliability*First*)	Wadsworth Electric & Communications (WEC)	NCR06020	RFC201100829	Settlement Agreement	On April 20, 2011, WEC, as a Distribution Provider, self-reported a violation of PRC-005-1 R2 to Reliability*First* prior to a scheduled compliance audit. WEC reported that it failed to maintain transmission relays as specified in its Program. Specifically, WEC failed to test all ten of its transmission relays within a five year interval. During the compliance audit, Reliability*First* found that all other protection system devices were tested and maintained within the intervals stated in WEC's Program. Reliability*First* determined that WEC violated the Standard by failing to include evidence of the last maintenance and testing, and documentation of the last date of testing and maintenance for relays.	PRC-005-1	R2	High	Severe	This violation posed a moderate risk to the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. WEC has alarming in place via a Supervisory Control and Data Acquisition (SCADA) system, which would immediately notify its Electric Division Headquarters and operations supervisors of any device failures. In addition, WEC completed the outstanding maintenance and testing in April 2011 and found no problems with the devices. WEC also indicated that it had tested the relays in November 2005.	06/18/2007 (date Standard became mandatory and enforceable)	04/05/2011 (date WEC completed testing and maintenance for the relays as defined by its Program)
Reliability*First* Corporation (Reliability*First*)	Wisconsin Electric Power Company (Wisconsin Electric)	NCR00951	RFC201000388	Settlement Agreement	From May 17, 2010 through May 21, 2010, Reliability*First* conducted a Compliance Audit of Wisconsin Electric during which it discovered a violation of PRC-005-1 R1. Reliability*First* determined that Wisconsin Electric, as a Distribution Provider (DP) and Generator Owner (GO), violated PRC-005-1 R1 by failing to include maintenance and testing intervals and a basis for those intervals for certain Protection System devices and by failing to include summaries of maintenance and testing procedures for certain Protection System devices, which are identified below. Wisconsin Electric's transmission Protection System maintenance and testing program for its DP function (DP Program) has been in place since January 2008 and Wisconsin Electric supplemented it on February 1, 2010. The 2008 version of the DP Program only included (i) maintenance and testing intervals and their basis for protective relays, and (ii) summaries of maintenance and testing procedures for protective relays. It did not include any maintenance and testing intervals and their basis or summaries of maintenance and testing procedures for the remaining Protection System devices. Specifically, this violation involved the omission of all of Wisconsin Electric's 243 transmission current sensing devices, 51 transmission station batteries and 111 transmission direct current control circuits, which constitutes 51.9% of its 779 total transmission Protection System devices. Wisconsin Electric's DP Program did not include voltage sensing devices or communication systems, since Wisconsin Electric has no DP voltage sensing devices and no DP communications systems. The 2010 version of Wisconsin Electric's DP Program required maintenance and testing on current transformers at installation only, thus the documentation did not include an acceptable maintenance and testing interval or an acceptable basis for that interval for current sensing devices. In addition, the 2010 version of Wisconsin Electric's DP Program did not include summaries of maintenance and testing procedures for current sensing devices. This violation involved the omission of all of Wisconsin Electric's transmission current sensing devices, which constitutes 31% of its 779 total transmission Protection System devices. Wisconsin Electric's generation Protection System maintenance and testing program for its GO function has been in place since 2006 (GO Program). Wisconsin Electric's GO Program documentation did not include any maintenance and testing interval or any basis for that interval for voltage and current sensing devices. In addition, the GO Program did not include summaries of maintenance and testing procedures for voltage and current sensing devices. This violation involved all of Wisconsin Electric's 72 generation voltage sensing devices and 408 generation current sensing devices, which constitute 28.6% of its total 1,678 generation Protection System devices.	PRC-005-1	R1	High	Severe	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. Although Wisconsin Electric's 2008 DP Program only included maintenance and testing intervals and their basis for protective relays, the audit team, as affirmed by Reliability*First* enforcement staff, confirmed that Wisconsin Electric performed maintenance and testing on its other Protection System devices in accordance with its 2010 DP Program throughout the time period of the violation. Although the 2010 program was not in effect for the entire duration of the violation, Wisconsin Electric had been performing maintenance and testing on all devices except sensing devices. The 2010 program memorialized Wisconsin Electric's maintenance and testing activities. Furthermore, although Wisconsin Electric did not include maintenance and testing intervals for voltage, since it had no DP sensing devices and only included it in its program for thoroughness, and current sensing devices in its DP or GO Programs, Wisconsin Electric's program documentation, which are maintenance and testing programs in place since June 18, 2007, indicates that it historically has tested its voltage and current sensing devices during the installation of its equipment and when it identifies problems with the equipment as part of its operations and upon visual inspections, consistent with the recommendations of the equipment manufacturers. Additionally, Wisconsin Electric routinely performs substation inspections, which included visual checks and infrared scans of the voltage and current sensing devices. Wisconsin Electric also verifies the voltage and current sensing devices' inputs into Protection System relays as part of those relays' periodic preventative maintenance and testing. Wisconsin Electric undertook these actions throughout the duration of the violation. In addition, Wisconsin Electric continuously monitors its voltage sensing devices for proper operation. An alarm alerts an operator who is on duty 24 hours a day to correct any potential issues before any loss of protection or interruption of service occurs. As a result of these actions, Wisconsin Electric found its voltage and current sensing devices in working condition throughout the duration of the violation.	6/18/2007 (When the Standard became mandatory and enforceable)	1/3/2011 (When Wisconsin Electric revised its DP Program to comply with the Standard); 2/18/2011 (Date Wisconsin Electric revised its GO Program to comply with the Standard)
Texas Reliability Entity, Inc. (Texas RE)	EDF Trading North America, LLC (EDF Trading)	NCR00551	TRE201100366	Settlement Agreement	On June 10, 2011, EDF Trading self-reported to Texas RE a possible violation of COM-002-2 R1. Texas RE determined that EDF Trading, as a Generator Operator (GOP), did not have communications available for addressing a real-time emergency condition, as required by the Standard. Specifically, during an Energy Emergency Alert (EEA) event on February 2, 2011, ERCOT ISO (the Balancing Authority and the Reliability Coordinator) issued a Verbal Dispatch Instruction (VDI) at 05:49 CPT via a hot line call to deploy 384 MW of ERCOT system Emergency Interruptible Load Service (EILS) system loads as part of a manual load shed to respond to the EEA. EDF Trading contends it did not receive the 05:49 CPT initial VDI via the hot line. ERCOT's evidence indicates that EDF Trading's phone was off the hook. EDF Trading reported that there was power to the phone system and operators were available to answer the phone. Texas RE determined that although EDF Trading had established communication links for addressing a real-time emergency condition, and although such communications were staffed, they were not available for addressing a real-time emergency situation on February 2, 2011.	COM-002-2	R1	High	Moderate	This violation posed a moderate risk to the reliability of the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS due to: (1) the small amount of interruptible load (7.4 MW, which is approximately 2% of ERCOT-wide EILS), and (2) the brief time period that EDF Trading was not available for answering the ERCOT communication link (approximately one hour). Additionally, once EDF Trading understood that EILS had been called by ERCOT, it successfully deployed its EILS pursuant to the ERCOT Protocols. The failure to follow the reliability directive in this case does not appear to be indicative of systemic issues adverse to system reliability.	2/2/2011 (Date of communications failure)	2/2/2011

Attachment A-1

January 31, 2012 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	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Texas Reliability Entity, Inc. (Texas RE)	EDF Trading North America, LLC (EDF Trading)	NCR00551	TRE201100392	Settlement Agreement	On July 22, 2011, EDF Trading self-reported to Texas RE a possible violation of TOP-006-1 R1. Texas RE determined that EDF Trading, as a Generator Operator (GOP), failed to inform its Host Balancing Authority and Transmission Operator of all generation resources available for use, as required by the Standard. Specifically, on February 2, 2011, Bayou Cogeneration Combustion Turbine No. 2 tripped at 01:54 CPT and was back on-line at 02:20. During the 26-minute interval between the turbine trip and when it was brought back on-line, EDF Trading failed to indicate that the unit status was "OFF" via the telemetering signal to ERCOT, the Host Balancing Authority and Transmission Operator, thus failing to inform of all generation resources available for use.	TOP-006-1	R1; R1.1	Medium	Severe	This violation posed a moderate risk to the reliability of the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because the generation at issue (75 MW nameplate rating) was unavailable for serving load for a 26-minute period regardless of whether the Standard was violated. The effect of failing to change the telemetered status to "OFF" was miscommunication. ERCOT operators believed that the ERCOT system had more operating reserve than they actually had. Although the ERCOT system was under stress (an Advisory was called at 02:47 and an Energy Emergency Alert (EEA) was called at 05:18), and there were limited and dwindling generation resources available, there were adequate operating reserves at the time regardless of the miscommunication and system frequency was stable at 59.97 Hz. Had the issue occurred during the EEA, it would have exacerbated the issues ERCOT was facing in the sense that miscommunication is inherently adverse to reliability. However, the resource would have been unavailable regardless of the quality of any communications.	2/2/2011 (Date of entity's failure to inform its Host Balancing Authority and Transmission Operator of all generation resources available for use)	2/2/2011
Western Electricity Coordinating Council (WECC)	Frederickson Power LP (FPWR)	NCR05164	WECC201103015	Settlement Agreement	On July 1, 2011, WECC notified FPWR that WECC was initiating the Self-Certification process for the reporting period of July 1, 2010 through August 31, 2011. Under this process, FPWR's Self-Certification submittal was due by September 20, 2011. On September 14, 2011, FPWR, as a Generator Operator (GOP), submitted a Self-Report addressing its noncompliance with VAR-002-1 R1 and on September 20, 2011, FPWR submitted its Self-Certification. WECC determined that the FPWR's Combustion Turbine Generator (CTG) was operating with the Automatic Voltage Regulator (AVR) in the wrong mode. Specifically, FPWR had been operating in VAR mode instead of Voltage Control mode from August 2, 2007 until January 12, 2011, when the unit was dispatched off-line. The computer interface has three generator mode options for the CTG: OFF, VAR (constant reactive power output), and PF (constant power factor). The OFF mode on the AVR computer interface is the correct mode for operating in voltage control mode. However, plant personnel believed the OFF position would remove the CTG AVR from service, so FPWR erroneously operated in VAR mode instead of Voltage Control/OFF mode. The change to the correct AVR mode was made during the period the unit was offline from January 12, 2011 to August 24, 2011. The unit was brought back online on August 24, 2011. FPWR notified its Transmission Operator (TOP), Bonneville Power Administration, of the change in AVR status on September 7, 2011. This is in violation of the Standard, which requires the GOP to operate in AVR mode and for the TOP to be notified of a change in AVR status within 30 minutes.	VAR-002-1	R1	Medium	Moderate	This violation posed a minimal risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS for several reasons. FPWR's net output of the combined cycle generation plant is based on the output of two distinct turbine-generators - the Combustion Turbine Generator (CTG) and the Steam Turbine Generator (STG). Although FPWR operated the CTG's AVR in VAR mode, the STG was consistently operated in the correct Voltage Control mode, thus reducing the potential risk that may have occurred through operating the CTG in an incorrect mode. Second, the output of the plant was always within the operating parameters defined by its transmission operator, BPA. Third, FPWR's operating personnel followed all directives given by BPA when deviations to the voltage schedule were required. FPWR's generation plant is a 249 MW facility with an annual operation of less than 50 percent.	8/2/2007 (when the Standard became mandatory and enforceable)	1/12/2011 (when FPWR's unit was dispatched off-line)
Western Electricity Coordinating Council (WECC)	Frederickson Power LP (FPWR)	NCR05164	WECC201103018	Settlement Agreement	On July 1, 2011, WECC notified FPWR that WECC was initiating the Self-Certification process for the reporting period of July 1, 2010 through August 31, 2011. Under this process, FPWR's Self-Certification submittal was due by September 20, 2011. On September 14, 2011, FPWR, as a Generator Operator (GOP), submitted a Self-Report addressing its noncompliance with VAR-002-1.1b R3 and on September 20, 2011, FPWR submitted its Self-Certification. WECC determined that the FPWR's Combustion Turbine Generator (CTG) was operating with the Automatic Voltage Regulator (AVR) in the wrong mode. Specifically, FPWR had been operating in VAR mode instead of Voltage Control mode from August 2, 2007 until January 12, 2011, when the unit was dispatched off-line. The change to the correct AVR mode was made during the period the unit was offline from January 12, 2011 to August 24, 2011. The unit was brought back online on August 24, 2011. FPWR notified its Transmission Operator (TOP), Bonneville Power Administration, of the change in AVR status on September 7, 2011. This is in violation of the Standard, which requires that the TOP be notified of a change in AVR status within 30 minutes.	VAR-002-1.1b	R3	Medium	High	This violation posed a minimal risk to the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS for several reasons. FPWR's net output of the combined cycle generation plant is based on the output of two distinct turbine-generators - the Combustion Turbine Generator (CTG) and the Steam Turbine Generator (STG). Although FPWR operated the CTG's AVR in VAR mode, the STG was consistently operated in the correct Voltage Control mode, thus reducing the potential risk that may have occurred through operating the CTG in an incorrect mode. Second, the output of the plant was always within the operating parameters defined by its transmission operator, BPA. Third, FPWR's operating personnel followed all directives given by BPA when deviations to the voltage schedule were required. FPWR's generation plant is a 249 MW facility with an annual operation of less than 50 percent.	8/24/2011 (when FPWR's unit was brought back online in a different AVR mode)	9/7/2011 (when FPWR notified BPA of the change in AVR status)
Western Electricity Coordinating Council (WECC)	Lower Valley Energy (LVE)	NCR05225	WECC201102432	Settlement Agreement	On February 14, 2011, LVE, as a Transmission Owner and Distribution Provider, self-certified noncompliance with PRC-005-1 R2 for failure to annually compare its current outputs to its System Control and Data Acquisition (SCADA) values, as required by its transmission Protection System maintenance and testing program. LVE should have compared its current outputs to its SCADA values by the end of August 2010. WECC determined that LVE maintained and performed most of the testing on its relevant protection equipment but failed to perform one test for comparing its current outputs to its SCADA values. LVE was in violation of this Standard for failing to maintain 100% of its current transformers (CTs) and potential transformers (PTs) within the defined intervals.	PRC-005-1	R2; R2.1	High	Severe	This violation posed a minimal risk to reliability of the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the BPS because LVE maintained and performed most of the testing on the relevant protection equipment and only failed to perform one test for comparing its current outputs to its SCADA values. Also, LVE's CTs and PTs are continuously monitored by its SCADA system. In addition, WECC considered the size of the entity, which is a 115 kV transmission system.	8/31/2010 (When LVE should have maintained and tested its CTs and PTs)	1/25/2011 (When LVE conducted maintenance and testing on the missed devices)
Western Electricity Coordinating Council (WECC)	NAES Corporation - Tracy (NAES-TR)	NCR05274	WECC201102436	Settlement Agreement	On January 20, 2011, NAES-TR, as a Generator Operator (GOP), submitted an Automatic Voltage Regulators (AVR) report for the fourth quarter of 2010 (Q4 2010), addressing a violation of VAR-STD-002a-1 WR1. Based on the record, WECC determined that NAES-TR did not operate its automatic control equipment in voltage control mode (VCM) for more than 92% of the hours during which its unit was on line for Q4 2010 and operated in power control mode instead. NAES-TR's operators were operating the AVR in a power control mode because they understood that its Transmission Operator, Pacific Gas and Electric Company, had instructed it to operate in this mode. However, WECC's regional Standard VAR-STD-002a-1 only allows the Transmission Operator to have the generator operate in a mode other than VCM under special conditions listed in the Standard, which were not applicable to this situation. As a result, WECC determined that NAES-TR violated VAR-STD-002a-1 WR1 for failure to operate its AVR in a VCM.	VAR-STD-002a-1	WR1	Lower	Level 4 Noncompliance	WECC determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because although NAES-TR did not operate in the proper mode, the generator involved (the Thermal Energy Development Partnership) is a synchronous biomass facility with a rated capacity of 23 MW, which is connected to a 115 kV transmission system. WECC took into consideration the entity's limited size and location and concluded that the entity has a very limited capacity to have more than a minimal impact on the reliability of the BPS.	10/1/2010 (When NAES-TR failed to operate its AVR in VCM, without an applicable exemption listed in the Standard)	4/21/2011 (When NAES-TR switched its AVR to the appropriate mode)

Attachment A-1

January 31, 2012 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	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Western Electricity Coordinating Council (WECC)	Sierra Pacific Power Company (SPPC), d/b/a NV Energy	NCR05390	WECC201102424	Settlement Agreement	On February 2, 2011, SPPC self-certified that although it met its quarterly battery testing intervals, it missed certain annual battery testing intervals set forth in SPPC's Protection System maintenance and testing program. The annual testing was established to address SPPC's obligations set forth in PRC-005-1 R2.1. On February 22, 2011, SPPC supplemented its Self-Certification with a Self-Report addressing additional batteries that were not tested in accordance with the annual interval set forth in SPPC's Protection System maintenance and testing program. During an on-site compliance audit of SPPC in March 2011, WECC subject matter experts (SMEs) reviewed the Self-Certification and Self-Report. The SMEs determined, pursuant to SPPC's Self-Certification and Self-Report, that SPPC failed to maintain 12 transmission station batteries and an additional 4 generation station batteries within the intervals defined in SPPC's Protection System maintenance and testing program. These 16 batteries represent fewer than 25 percent of all of SPPC's Protection System batteries. SPPC is subject to this Standard because it is registered with NERC as a Transmission Owner, Distribution Provider and Generator Owner.	PRC-005-1	R2; R2.1	High	Lower	SPPC conducts quarterly station battery inspections. This violation relates to SPPC's failure to conduct its annual (not to exceed 16 month) scheduled battery tests. Although SPPC missed annual testing, it did not miss its quarterly battery inspections. SPPC personnel are aware of the condition of the batteries based on the quarterly inspections and would note and take action if SPPC detected a potential battery failure. Further, the batteries support only a small fraction of SPPC's transmission Protection System and an even smaller fraction of SPPC's generation Protection System. In addition, SPPC system protection engineers regularly review the battery maintenance records for consistency. For these reasons, WECC determined this violation did not pose a serious or substantial risk and posed minimal risk to the reliability of the bulk power system.	12/10/2009 (Date of first missed interval for battery maintenance and testing)	2/17/2011 (When SPPC tested its batteries pursuant to the Protection System maintenance and testing program)
Western Electricity Coordinating Council (WECC)	Sierra Pacific Power Company (SPPC), d/b/a NV Energy	NCR05390	WECC201102425	Settlement Agreement	From March 14, 2011 through March 25, 2011, WECC conducted an on-site compliance audit of SPPC (Audit). The Audit team clarified with SPPC that station batteries at Downs, Muller, Northstar, Anaconda Yerington and Tahoe City stations, which support SPPC's Under Frequency Load Shedding (UFLS) Protection System, were not in the UFLS program. Therefore, the Audit team determined SPPC's UFLS program did not include all UFLS station batteries and was a possible violation of PRC-008-0 R1. The Audit team noted that WECC had previously audited SPPC and did not identify a possible violation of PRC-008-0 R1. The Audit team forwarded its findings to Enforcement. Enforcement reviewed the Audit findings and determined SPPC's failure to identify UFLS station batteries in its UFLS maintenance and testing program, including a schedule for testing, is a violation of PRC-008-0 R1. SPPC is subject to this Standard as a Transmission Owner and Distribution Provider.	PRC-008-0	R1	Medium	Moderate	Failure to ensure periodic maintenance of UFLS station batteries could lead to a failure of a specific UFLS relay. However, although SPPC did not identify station batteries in its UFLS program it did maintain and test UFLS station batteries as part of its routine station battery maintenance and testing. Further, only 5 of the 16 battery stations supporting UFLS were not addressed in SPPC's PRC-005 Protection System maintenance and testing program. SPPC adequately identified and addressed all other components of its UFLS Protection System in its UFLS program. For these reasons, WECC determined this violation posed minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS).	6/18/2007 (When the Standard was enforceable)	5/31/2011 (Mitigation Plan completion)
Western Electricity Coordinating Council (WECC)	Sierra Pacific Power Company (SPPC), d/b/a NV Energy	NCR05390	WECC201102426	Settlement Agreement	On February 2, 2011, SPPC self-certified possible noncompliance with PRC-008-0 R2. WECC subject matter experts (SMEs) reviewed the Self-Certification and associated evidence during an on-site compliance audit of SPPC in March 2011. The SMEs reviewed maintenance records for all SPPC Under Frequency Load Shedding (UFLS) equipment and determined SPPC appropriately self-certified noncompliance with this requirement. The SMEs also determined SPPC failed to maintain or test one UFLS relay (out of 22 total) within the interval defined in SPPC's UFLS maintenance and testing plan. The SMEs determined this was a possible violation of PRC-008-0 R2. The SMEs forwarded the Self-Certification and the SMEs' findings to Enforcement. Enforcement reviewed the Self-Certification and the SME's findings. Enforcement determined SPPC did not maintain and test a UFLS relay at the Fort Churchill substation within the interval defined within SPPC's UFLS maintenance and testing plan. Accordingly, Enforcement determined SPPC's failure to implement its UFLS program is a violation of PRC-008-0 R2. SPPC is subject to this Standard as a Transmission Owner and Distribution Provider.	PRC-008-0	R2	Medium	Lower	SPPC failed to test one UFLS relay out of 22 total UFLS relays. Thus, this violation is limited to a small fraction of the SPPC UFLS protective devices. Further, SPPC has a six-year interval for these devices and tested the relay six months beyond the defined interval. Such a testing delay in relation to the number of total devices does not represent a significant deviation from SPPC's UFLS program, and it is unlikely the relay would deteriorate or have its settings inadvertently misconfigured within the six-month delay in maintenance and testing. For these reasons, WECC determined this violation posed minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS).	5/6/2010 (Date of first missed interval for UFLS maintenance and testing)	12/23/2010 (When SPPC tested its UFLS relay pursuant to the UFLS program)
Western Electricity Coordinating Council (WECC)	Sierra Pacific Power Company (SPPC), d/b/a NV Energy	NCR05390	WECC201102438	Settlement Agreement	From March 14, 2011 through March 25, 2011, WECC conducted an on-site compliance audit of SPPC (Audit). During and prior to the Audit, the Audit team reviewed SPPC's *Special Protection System Maintenance and Testing* Version 3, dated February 14, 2011 (SPS Plan). Of the six Special Protection Systems identified in SPPC's SPS Plan, the Audit team identified two Special Protection Systems where SPPC failed to maintain and test associated station batteries within the intervals defined in the SPS Plan. SPPC could not demonstrate that it maintained and tested the station batteries at the Rusty Spike station, associated with the Airport 173 Line Thermal Overload SPS, and the Eight Mile station, associated with the Eight Mile Creek Overload SPS, within the intervals defined in the SPS Plan. These two batteries were already self-reported as out of compliance in PRC-005, but were not self-reported again in PRC-017. Therefore, the Audit team determined SPPC had a possible violation of PRC-017-0 R2. The Audit team forwarded its findings to Enforcement. Enforcement reviewed the Audit findings and determined SPPC's failure to maintain and test station batteries at the Rusty Spike and Eight Mile facilities within the intervals defined in SPPC's Special Protection System maintenance and testing program resulted in SPPC not implementing its program. For these reasons, Enforcement determined SPPC had a violation of PRC-017-0 R2. SPPC is subject to this Standard as a Transmission Owner, Generator Owner and Distribution Provider.	PRC-017-0	R2	Lower	Lower	SPPC conducts quarterly station battery inspections. This violation relates to SPPC's failure to conduct its annual (not to exceed 16 month) scheduled SPS battery tests. Although SPCC did not perform annual inspection, SPPC did not miss its quarterly battery inspections. SPPC personnel are aware of the condition of the batteries based on the quarterly inspections and would note and take action if SPPC detected a potential battery failure. The violation only relates to two of SPPC's six Special Protection Systems. Further, the violation is associated with station batteries whose battery maintenance records receive regular review from protection engineers. For these reasons, WECC determined this violation posed minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS).	7/17/2010 (When SPPC missed testing station batteries pursuant to its program)	3/23/2011 (Mitigation Plan completion)

Attachment A-1
January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/ Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$0	Self- Report	The entity mitigated the issue by performing the following activities: (1) The entity enhanced its Facility Rating Methodology to include flexibility to account for cold weather conditions and the specific characteristics of autotransformers and other power system equipment to address real-time conditions. A new Methodology was developed by entity operations to include normal and emergency winter Ratings; (2) The entity also updated its operations procedures to include actions to take in cold weather conditions as they relate to the enhanced Rating Methodology. System operations procedures were updated to include a specific list of actions to take in anticipation of and during cold weather conditions. The procedures include a process for utilizing winter Ratings including but not limited with respect to the autotransformer in question. The procedures also include a process where the system operator can review and modify as appropriate, specific emergency limits based on real-time information; (3) Furthermore, the entity provided training to operators, which included a review of the following: (a) the January 13, 2011 event in detail; (b) its new Rating Methodology with operators, especially cold weather normal and emergency Ratings; (c) the modified operations procedures; (d) appropriate standards, responsibilities and expectations of transmission operators for SOLs and other equipment overloads, with emphasis on cold weather operations; and (e) remedial action plans with emphasis on actions during cold weather operations.	6/1/2011	10/24/2011	Neither Admits nor Denies	The entity has a documented internal compliance program (ICP) which was in place at the time of the violation, which was considered a mitigating factor in the penalty determination, that was recently reviewed by FRCC to verify the program included violation mitigation, corrective action processes, internal controls, upper management involvement and a structure that encourages a culture of compliance within the organization. The evaluation determined that many of the key elements were established and implemented to ensure the entity maintains a robust internal compliance program. FRCC also took into account as a mitigating factor the fact that the registered entity also undertook voluntary and appropriate measures pursuant to the NERC Event Analysis program to address the related event. The registered entity performed all of the steps in the program including an internal compliance evaluation and a self-report. In addition, FRCC considered the fact that there was controlled manual load shed (to bring loading below the then established SOL) which was considered in the penalty determination.
$15,000	Self-Report	AE Supply will reinforce the importance of timely reporting of changes in AVR status to all AE Supply power station management. Additionally, AE Supply will develop and conduct AVR status training for AE Supply power station personnel, emphasizing the process and procedures to follow in the event of a status or capability change on any generator reactive power resource. AE Supply also will conduct training on reporting AVR status for real-time operating personnel responsible for notifying the TOP. Finally, AE Supply will revise its power station outage startup procedures to include verification that the AVR is in automatic before startup begins.	3/31/2012 (Approved Date)	TBD	Agrees/Stipulates	AE Supply is a wholly-owned, indirect subsidiary of FirstEnergy Corp. (FirstEnergy). Prior to February 25, 2011, AE Supply was a wholly-owned subsidiary of Allegheny Energy, Inc. (Allegheny), a public utility company. On February 25, 2011, FirstEnergy acquired Allegheny and its affiliates, including AE Supply. Of the nine occasions constituting the violation of VAR-002-1.1a R3, five occurred prior to FirstEnergy's February 25, 2011 acquisition of Allegheny and its registered affiliates. Therefore, Reliability*First* considered both FirstEnergy's and Allegheny's respective compliance programs and cultures of compliance as mitigating factors in determining the penalty amount. Allegheny had a documented internal compliance program, in effect at the time of the violation which established the goals, structure, responsibilities and processes for achieving full compliance with Reliability Standards. Allegheny distributed its compliance program on the internal Allegheny website. Allegheny continually reviewed its compliance program, and conducted training, as required, to introduce new compliance requirements or to reinforce existing requirements. AE Supply conducted an internal review of 50% of all applicable standards on a biennial schedule. FirstEnergy's *FERC Reliability and Compliance Policy* addresses all Reliability Standards. FirstEnergy updates the policy and procedures as necessary and distributes the policy to FirstEnergy and affiliate employees. The compliance program includes engagement and support of senior management.
$20,000 (for RFC201100944, RFC201100945, RFC201100946, and RFC201100947)	Self-Report	On June 27, 2011, BSPP submitted to Reliability*First* a Mitigation Plan addressing the alleged violation of FAC-008-1 R1. In accordance with the Mitigation Plan, BSPP (1) documented its formal rating Methodology pursuant to the requirements of the standard and (2) included terminal equipment in its Methodology and all of the factors listed in Requirements R1.1 - R1.3.5.	4/19/2011	11/28/2011	Neither Admits nor Denies	Reliability*First* considered the following mitigating factors when determining the penalty amount. First, certain aspects of BSPP's compliance program were determined by Reliability*First* to be mitigating factors. BSPP distributes its compliance program to employees who have direct or indirect responsibility for compliance. BSP employees and corporate team members regularly attend NERC and regional workshops and conferences. BSPP's reliability compliance officer, the Vice President, Operations, reports to the President and CEO, Operations. The President and CEO, Operations, has direct access to both the Chairman and CEO of Tenaska, Inc. Additionally, the Vice President, Operations, attends regular meetings with the President and CEO, Operations, as well as the Board of Stakeholders and is encouraged to discuss reliability and compliance matters with them. BSPP assigned the responsibility for ensuring independent program management to the Vice President, Transmission. The Vice President, Transmission, does not report to the President and CEO, Operations, which enhances the independence in managing the compliance program. BSPP conducts internal audits as well as reviews and authorizes the compliance program semi-annually. Reliability*First* determined that there were no aggravating factors in determining the penalty amount.

Attachment A-1
January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/ Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$20,000 (for RFC201100944, RFC201100945, RFC201100946, and RFC201100947)	Self-Report	On June 27, 2011, BSPP submitted to Reliability*First* a Mitigation Plan addressing the alleged violation of FAC-009-1 R1. In accordance with the Mitigation Plan, BSPP utilized its updated Methodology to develop Facility Ratings pursuant to the Standard.	4/19/2011	11/28/2011	Neither Admits nor Denies	Reliability*First* considered the following mitigating factors when determining the penalty amount. First, certain aspects of BSPP's compliance program were determined by Reliability*First* to be mitigating factors. BSPP distributes its compliance program to employees who have direct or indirect responsibility for compliance. BSP employees and corporate team members regularly attend NERC and regional workshops and conferences. BSPP's reliability compliance officer, the Vice President, Operations, reports to the President and CEO, Operations. The President and CEO, Operations, has direct access to both the Chairman and CEO of Tenaska, Inc. Additionally, the Vice President, Operations, attends regular meetings with the President and CEO, Operations, as well as the Board of Stakeholders and is encouraged to discuss reliability and compliance matters with them. BSPP assigned the responsibility for ensuring independent program management to the Vice President, Transmission. The Vice President, Transmission, does not report to the President and CEO, Operations, which enhances the independence in managing the compliance program. BSPP conducts internal audits as well as reviews and authorizes the compliance program semi-annually. Reliability*First* determined that there were no aggravating factors in determining the penalty amount.
$20,000 (for RFC201100944, RFC201100945, RFC201100946, and RFC201100947)	Self-Report	On June 27, 2011, BSPP submitted to Reliability*First* a Mitigation Plan addressing the alleged violation of PRC-005-1 R1. In accordance with the Mitigation Plan, BSPP included in its documented Program (1) maintenance and testing intervals and the basis for those intervals, (2) a summary of maintenance and testing procedures for its Protection System devices, and (3) a new basis for maintenance and testing of its voltage and current sensing devices. The updated program has clearly defined procedures for the maintenance and testing of DC Control Circuitry, CTs and PTs.	9/26/2011	1/31/2012	Neither Admits nor Denies	Reliability*First* considered the following mitigating factors when determining the penalty amount. First, certain aspects of BSPP's compliance program were determined by Reliability*First* to be mitigating factors. BSPP distributes its compliance program to employees who have direct or indirect responsibility for compliance. BSP employees and corporate team members regularly attend NERC and regional workshops and conferences. BSPP's reliability compliance officer, the Vice President, Operations, reports to the President and CEO, Operations. The President and CEO, Operations, has direct access to both the Chairman and CEO of Tenaska, Inc. Additionally, the Vice President, Operations, attends regular meetings with the President and CEO, Operations, as well as the Board of Stakeholders and is encouraged to discuss reliability and compliance matters with them. BSPP assigned the responsibility for ensuring independent program management to the Vice President, Transmission. The Vice President, Transmission, does not report to the President and CEO, Operations, which enhances the independence in managing the compliance program. BSPP conducts internal audits as well as reviews and authorizes the compliance program semi-annually. Reliability*First* determined that there were no aggravating factors in determining the penalty amount.
$20,000 (for RFC201100944, RFC201100945, RFC201100946, and RFC201100947)	Self-Report	On June 27, 2011, BSPP submitted to Reliability*First* a Mitigation Plan addressing the alleged violation of PRC-005-1 R2. In accordance with the Mitigation Plan, BSPP (1) updated its Program to include defined procedures for maintenance and testing of its DC Control Circuits and (2) conducted maintenance and testing of its DC Control Circuits pursuant to its Program.	9/26/2011	1/31/2012	Neither Admits nor Denies	Reliability*First* considered the following mitigating factors when determining the penalty amount. First, certain aspects of BSPP's compliance program were determined by Reliability*First* to be mitigating factors. BSPP distributes its compliance program to employees who have direct or indirect responsibility for compliance. BSP employees and corporate team members regularly attend NERC and regional workshops and conferences. BSPP's reliability compliance officer, the Vice President, Operations, reports to the President and CEO, Operations. The President and CEO, Operations, has direct access to both the Chairman and CEO of Tenaska, Inc. Additionally, the Vice President, Operations, attends regular meetings with the President and CEO, Operations, as well as the Board of Stakeholders and is encouraged to discuss reliability and compliance matters with them. BSPP assigned the responsibility for ensuring independent program management to the Vice President, Transmission. The Vice President, Transmission, does not report to the President and CEO, Operations, which enhances the independence in managing the compliance program. BSPP conducts internal audits as well as reviews and authorizes the compliance program semi-annually. Reliability*First* determined that there were no aggravating factors in determining the penalty amount.

Attachment A-1
January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/ Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$0	Compliance Audit	During the Compliance Audit, Reliability*First* determined Buckeye Power mitigated the violation of the Standard when it implemented the current version of the Facility Ratings Methodology on December 18, 2009.	12/18/2009	7/25/2011	Agrees/ Stipulates	Reliability*First* considered Buckeye Power's formal internal compliance program (ICP), in effect at the time of the violation, as a mitigating factor. The ICP resides within the Power Supply division and was widely disseminated to all individuals within this division through small workshops, training by consultants, emails, 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 ICP resulted in expanding the scope of compliance activities to include more staff, including an additional consultant.
$5,000	Self-Report	WEC entered into an agreement with FirstEnergy Corporation (FirstEnergy), whereby FirstEnergy agreed to perform maintenance and testing on the relays for WEC's two 138 kV transmission lines. FirstEnergy completed this testing on behalf of WEC on April 5, 2011. WEC has also established a schedule with FirstEnergy to ensure timely future testing and maintenance of protection system devices.	4/5/2011	8/25/2011	Agrees/Stipulates	Reliability*First* considered certain aspects of WEC's Internal Compliance Program (ICP), which was in effect at the time of the violation, as mitigating factors when assessing the penalty. WEC's employees attend reliability-focused seminars, workshops, and conference calls, and WEC has identified individuals in its organization to be responsible for compliance with NERC standards. Reliability issues are communicated to staff at weekly staff meetings, and WEC conducted an internal audit in 2010. Since the Self-Report was submitted in anticipation of an audit, WEC did not receive the credit normally given for Self-Reports.
$10,000	Compliance Audit	Wisconsin Electric revised its DP Program and its GO Program to include maintenance and testing intervals for voltage and current sensing devices. The 2010 version of Wisconsin Electric's DP Program had been revised to include maintenance and testing intervals, their basis and summaries for transmission station batteries.	2/18/2011	1/25/2012	Neither Admits nor Denies	Reliability*First* considered as a mitigating factor certain aspects of Wisconsin Electric's internal compliance culture. Wisconsin Electric has an internal compliance program, which was in effect at the time of the violation which consists of the Federal Regulatory Affairs and Policy (FRAP) group. The FRAP group developed and implemented the Federal Energy Regulatory Compliance Program to assure and demonstrate compliance with the FERC electric regulations including the NERC Reliability Standards. The FRAP group also assists in the development and documentation of the necessary compliance processes and helps educate Wisconsin Electric individuals responsible for executing the compliance process. In addition, Wisconsin Electric requires all employees to annually certify their review and understanding of corporate policies, including the Code of Business Conduct. The Corporate Compliance Officer, who is the Corporate Secretary and Associate General Counsel, has independent access to the Audit and Oversight Committee of the Board of Directors, as well as to the CEO and Chairman of the Board of Wisconsin Energy Corporation. In addition, senior management approves policies, procedures, self-certifications, and data submittals, and receives quarterly reports on the level of FERC and NERC compliance in their respective areas.
$21,000 (for TRE201100366 and TRE201100392)	Self-Report	On June 6, 2011, EDF Trading submitted to Texas RE a Mitigation Plan to address the violation of COM-002-2 R1. In accordance with the Mitigation Plan, EDF Trading has completed the following: (1) implemented a procedure requiring the EDF Trading real-time desk operator to check the phone status at the beginning of his/her shift, assuming system conditions are normal; (2) implemented a procedure to have APX (EDF Trading's energy management service provider) alarm the EDF Trading real-time desk upon receipt of a hot line call to APX; (3) implemented an alarm upon the receipt of Market Information System (MIS, an ERCOT computer system) notification of deployments of EILS as well as other VDIs and emergency notices; (4) implemented monitoring and storing channel bank interface status to provide real-time status of "hook" indicators on the hot line phone analog channels; and (5) implemented monitoring and storing the condition of the ERCOT trunk interface to the hot line phone gear.	12/31/2011	1/4/2012	Neither Admits nor Denies	EDF Trading's internal compliance program, in place at the time of the violation, was considered by Texas RE to be a mitigating factor in the penalty determination. EDF Trading maintains and regularly updates a written compliance program. EDF Trading relies on the written compliance program and desk/department heads to ensure compliance with NERC standards. The written compliance program is both widely distributed and available to all employees. EDF Trading has engaged a third-party consultant to assist in the ongoing development of formal compliance policies. In addition, EDF Trading has hired outside counsel to assist in actively monitoring changing regulatory requirements. EDF Trading reviews NERC standards and requirements approximately every six months. EDF Trading engages in a regular compliance training program. New employees are assigned a mentor for training for approximately one month after hire. EDF Trading has a named and staffed director of regulatory affairs who is charged with overseeing implementation of its compliance program. The director of regulatory affairs reports to the senior vice president and general counsel, who has the overall responsibility for reliability compliance. Both the senior VP and general counsel and the senior vice president of trading and risk have independent access to the CEO.

Attachment A-1

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/ Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$21,000 (for TRE201100366 and TRE201100392)	Self-Report	On June 6, 2011, EDF Trading submitted to Texas RE a Mitigation Plan to address the violation of TOP-006-1 R1. In accordance with the Mitigation Plan, EDF Trading has implemented automated processes with APX (EDF Trading's energy management service provider) to update resource status upon change in telemetered or received elements or notices.	1/1/2012	1/4/2012	Neither Admits nor Denies	EDF Trading's internal compliance program, in place at the time of the violation, was considered by Texas RE to be a mitigating factor in the penalty determination. EDF Trading maintains and regularly updates a written compliance program. EDF Trading relies on the written compliance program and desk/department heads to ensure compliance with NERC standards. The written compliance program is both widely distributed and available to all employees. EDF Trading has engaged a third-party consultant to assist in the ongoing development of formal compliance policies. In addition, EDF Trading has hired outside counsel to assist in actively monitoring changing regulatory requirements. EDF Trading reviews NERC standards and requirements approximately every six months. EDF Trading engages in a regular compliance training program. New employees are assigned a mentor for training for approximately one month after hire. EDF Trading has a named and staffed director of regulatory affairs who is charged with overseeing implementation of its compliance program. The director of regulatory affairs reports to the senior vice president and general counsel, who has the overall responsibility for reliability compliance. Both the senior VP and general counsel and the senior vice president of trading and risk have independent access to the CEO.
$1,000 (for WECC201103015 and WECC201103018)	Self-Certification	FPWR submitted a mitigation plan on November 1, 2011 with a completion date of September 7, 2011. To mitigate this violation FPWR performed the following: 1. Frederickson Power has applied the General Electric TIL 1731 on May 5, 2010 to update the control screen interface as evidenced by the completed work order. 2. The site manager at the Frederickson plant has contacted the Bonneville Power Administration (BPA) to review the voltage schedule for Frederickson Power/South Tacoma Switchyard. He has confirmed documentation of the proper control ranges and ensured Frederickson Power has maintained the voltage schedule. 3. Frederickson Power has revised the startup procedures to clarify the correct CTG AVR operation on September 7,2011. 4. Frederickson Power has re-trained operating personnel on startup procedures and circulated an email summarizing the procedural changes September 7, 2011.	9/7/2011	1/26/2012	Does Not Contest	WECC determined there were no aggravating factors that would warrant a penalty higher than the recommended penalty. Specifically, FPWR did not have repeat violations of this Standard nor relevant negative compliance history. FPWR did not fail to complete an applicable compliance directives. Additionally, there was no evidence of any attempt by FPWR to conceal the violation, or any evidence that FPWR's violation was intentional.
$1,000 (for WECC201103015 and WECC201103018)	Self-Certification	FPWR submitted a mitigation plan on November 1, 2011 with a completion date of September 7, 2011. To mitigate this violation FPWR performed the following: 1. Frederickson Power has applied the General Electric TIL 1731 on May 5, 2010 to update the control screen interface as evidenced by the completed work order. 2. The site manager at the Frederickson plant has contacted the Bonneville Power Administration (BPA) to review the voltage schedule for Frederickson Power/South Tacoma Switchyard. He has confirmed documentation of the proper control ranges and ensured Frederickson Power has maintained the voltage schedule. 3. Frederickson Power has revised the startup procedures to clarify the correct CTG AVR operation on September 7,2011. 4. Frederickson Power has re-trained operating personnel on startup procedures and circulated an email summarizing the procedural changes September 7, 2011.	9/7/2011	1/26/2012	Does Not Contest	WECC determined there were no aggravating factors that would warrant a penalty higher than the recommended penalty. Specifically, FPWR did not have repeat violations of this Standard nor relevant negative compliance history. FPWR did not fail to complete an applicable compliance directives. Additionally, there was no evidence of any attempt by FPWR to conceal the violation, or any evidence that FPWR's violation was intentional.
$7,500	Self-Certification	On March 23, 2011, LVE submitted a Mitigation Plan, stating that it had addressed its noncompliance with this Standard by performing the missing CT and PT device testing. In addition, LVE updated its tracking spreadsheet to include the testing procedures that were missed.	4/26/2011	12/21/2011	Agrees/ Stipulates	WECC did not review an internal compliance program (ICP) for LVE and therefore, this factor had no impact on the penalty determination. WECC considered that LVE met its first Mitigation Plan milestone in January 2011 to perform maintenance and testing (essentially mitigating the instant violation), however LVE met its preventative measure milestone (to update its tracking spreadsheet) 34 days after the approved date. WECC determined that no adjustments to the penalty were warranted.
$500	Self-Report	NAES-TR submitted its Mitigation Plan to WECC on 6/13/2011, with a completion date of 5/12/2011. NAES-TR switched its AVR into the appropriate mode on 4/21/2011.	4/21/2011	12/29/2011	Agrees/Stipulates	WECC considered that there were no aggravating factors.

Attachment A-1

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

(NON-CIP Violations)

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Agrees/ Stipulates," "Neither Admits nor Denies," or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$16,400 (for WECC201102424, WECC201102425, WECC201102426, WECC201102438)	Self-Certification	On May 5, 2011, SPPC submitted a Mitigation Plan to address this violation. In the Mitigation Plan, SPPC identified the cause of the violation as "SPPC identified 12 substation batteries as being out of compliance on their maintenance intervals, additionally SPPC self-reported 4 plant batteries as being out of compliance on their maintenance intervals when discovered." SPPC clarified that it missed the 16 batteries "due to a combination of human error, incorrect data from an old database, and lack of awareness." As a result of this observation, SPPC trained its employees "on NERC Compliance [including] the nature of compliance as well as the maintenance intervals." To avoid confusion, going forward, SPPC will ensure the date listed on the test results documentation is the date the actual test was performed (rather than the date the results were downloaded off the test instrument). SPPC also migrated its old database to a new database and configured the database to target Protection Systems, in this case batteries, subject to PRC-005. With the data migration, SPPC removed the necessity for manual, human oversight regarding the intervals.	4/4/2011	1/10/2012	Neither Admits nor Denies	Although there is a violation of this Reliability Standard on the part of an SPPC affiliate, Enforcement determined the SPPC affiliate violation occurred concurrent to a previous SPPC violation. Enforcement considered as an aggravating factor that this violation is SPPC's second assessed violation of PRC-005-1 R2. WECC evaluated SPPC's internal compliance program (ICP) and found the following: SPPC has a fully documented ICP that has been reviewed and approved by general counsel who also serves as its chief compliance officer. SPPC's oversight position is identified and staffed, and is supervised at a high level within the company. The ICP oversight position has direct access to the CEO and board of directors and SPPC operates and manages the ICP independently from personnel responsible for compliance with the Reliability Standards. The ICP has sufficient staff and an adequate budget, SPPC senior management support and participate in the ICP, and SPPC's ICP has an annual review cycle. Based on these findings, WECC concluded that SPPC has an effective compliance culture.
$16,400 (for WECC201102424, WECC201102425, WECC201102426, WECC201102438)	Compliance Audit	On May 31, 2011, SPPC submitted a Mitigation Plan to address this violation. SPPC added UFLS station batteries previously not included to its UFLS program. SPPC updated it documented procedure on PRC-008 to include the newly identified batteries.	5/31/2011	6/27/2011	Neither Admits nor Denies	Enforcement considered that WECC's 2009 audit of SPPC did not identify a possible violation of PRC-008-1 R1 and WECC had previously indicated to SPPC that it was deemed compliant with this requirement. SPPC did not substantially alter its program with regard to UFLS station batteries since the 2009 audit and PRC-008-1 R1 had not been modified since WECC last deemed SPPC to be compliant with the standard. SPPC relied in good faith, in part, on the 2009 audit finding as SPPC implemented its UFLS program. WECC evaluated SPPC's internal compliance program (ICP) and found the following: SPPC has a fully documented ICP that has been reviewed and approved by general counsel who also serves as its chief compliance officer. SPPC's oversight position is identified and staffed, and is supervised at a high level within the company. The ICP oversight position has direct access to the CEO and board of directors and SPPC operates and manages the ICP independently from personnel responsible for compliance with the Reliability Standards. The ICP has sufficient staff and an adequate budget, SPPC senior management support and participate in the ICP, and SPPC's ICP has an annual review cycle. Based on these findings, WECC concluded that SPPC has an effective compliance culture.
$16,400 (for WECC201102424, WECC201102425, WECC201102426, WECC201102438)	Self-Certification	On May 5, 2011, SPPC submitted a Mitigation Plan to address this violation. In the Mitigation Plan, SPPC identified the cause of the violation as SPPC's "one UF relay (Ft Churchill 130) was self-certified as being out of compliance on its maintenance interval." WECC confirmed that SPPC tested the relay on December 23, 2010. SPPC ensured all relays were added to its automated tracking system, PowerBase, removing the necessity for a manual or human reference. SPPC also updated its PRC-008 policy by modifying its maintenance intervals for UFLS relays to match the maintenance interval associated with SPPC's PRC-005 program.	3/28/2011	6/27/2011	Neither Admits nor Denies	WECC evaluated SPPC's internal compliance program (ICP) and found the following: SPPC has a fully documented ICP that has been reviewed and approved by general counsel who also serves as its chief compliance officer. SPPC's oversight position is identified and staffed, and is supervised at a high level within the company. The ICP oversight position has direct access to the CEO and board of directors and SPPC operates and manages the ICP independently from personnel responsible for compliance with the Reliability Standards. The ICP has sufficient staff and an adequate budget, SPPC senior management support and participate in the ICP, and SPPC's ICP has an annual review cycle. Based on these findings, WECC concluded that SPPC has an effective compliance culture.
$16,400 (for WECC201102424, WECC201102425, WECC201102426, WECC201102438)	Compliance Audit	On May 5, 2011, SPPC submitted a Mitigation Plan to address this violation. In the Mitigation Plan, SPPC stated SPPC personnel "is now aware that non-compliance should be reported under all standards the piece of equipment in violation is found under" and noted that SPPC is addressing the batteries "in the Mitigation Plan [submitted] under PRC-005-1 R2."	3/23/2011	1/10/2012	Neither Admits nor Denies	WECC evaluated SPPC's internal compliance program (ICP) and found the following: SPPC has a fully documented ICP that has been reviewed and approved by general counsel who also serves as its chief compliance officer. SPPC's oversight position is identified and staffed, and is supervised at a high level within the company. The ICP oversight position has direct access to the CEO and board of directors and SPPC operates and manages the ICP independently from personnel responsible for compliance with the Reliability Standards. The ICP has sufficient staff and an adequate budget, SPPC senior management support and participate in the ICP, and SPPC's ICP has an annual review cycle. Based on these findings, WECC concluded that SPPC has an effective compliance culture.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Midwest Reliability Organization (MRO)	Unidentified Registered Entity 1 (MRO_URE1)	NCRXXXXX	MRO201100260	Notice of Confirmed Violation	MRO conducted a CIP Spot Check of MRO_URE1. MRO determined that MRO_URE1 did not provide sufficient evidence reflecting the use of appropriate test procedures to ensure that new Cyber Assets (CAs) and significant changes to CAs within the Electronic Security Perimeter (ESP) do not adversely affect existing cyber security controls. Specifically, MRO_URE1 periodically utilized an intermediate anti-virus server to download anti-virus signature and security patch updates for the CAs within the ESP. MRO_URE1 failed to test the server each time it was reintroduced into the ESP, because it did not consider the anti-virus server to be a "new" CA each time it reconnected to the ESP, and therefore did not have evidence demonstrating that appropriate test procedures had been followed. MRO_URE1 indicated that this violation was due to an insufficient understanding among responsible MRO_URE1 personnel of the criteria for defining and classifying non-critical CAs residing within the ESP.	CIP-007-1	R1	Medium	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS). This violation did not pose a serious or substantial risk to the reliability of the bulk power system because: (1) although the introduction of new CAs or the modification of existing CAs without verification that cyber security controls are functioning properly can put many or all Critical Cyber Assets in a given ESP at risk and jeopardize the proper functioning of existing CAs, the intermediate anti-virus server utilized by MRO_URE1 was configured as a hardened, single-purpose device, thus reducing the risk of compromise by malware or other exploits; (2) MRO_URE1 tested anti-malware signatures and security patch updates in a development environment prior to introduction to the ESP; and (3) the intermediate anti-virus server was not connected simultaneously to the ESP and the MRO_URE1 corporate network.	The date MRO_URE1 was required to comply with the Reliability Standard.	Mitigation Plan completion
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000305	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a possible violation of CIP-004-1 R2. Reliability*First* determined that RFC_URE1 did not ensure that individuals with cyber or unescorted physical access to Critical Cyber Assets (CCAs) received training within 90 calendar days of receiving authorization or annual training, pursuant to CIP-004-1 R2. Six months later, RFC_URE1 provided additional information to supplement the information contained in the first Self-Report and identified another possible violation of the Standard. First, RFC_URE1 did not train 39 individuals within 90 days of granting them access to CCAs, as required by CIP-004-1 R2.1.3. Specifically, RFC_URE1 did not provide the requisite CIP training to 33 of the 39 individuals within 90 days of authorization. Out of the 33 individuals not trained within 90 days: 3 were RFC_URE1 employees with cyber access to CCAs; 12 were RFC_URE1 employees with unescorted physical access to CCAs; two were contractors with cyber access to CCAs; and 16 were contractors with authorized unescorted physical access. In addition, RFC_URE1 did not provide any CIP training to six of the 39 individuals with access to CCAs. One of the six individuals was an RFC_URE1 employee with cyber access to CCAs, three of the six were RFC_URE1 employees with unescorted physical access to CCAs, and two of the six individuals were contractors with unescorted physical access to CCAs. Second, RFC_URE1 did not administer annual CIP training sessions for 183 individuals as required by CIP-004-1 R2.3. Of the 183 individuals: 61 of these individuals were RFC_URE1 employees with cyber access to CCAs; eight were RFC_URE1 employees with both cyber and unescorted physical access to CCAs; 66 were employees with only unescorted physical access to CCAs; and 48 were contractors with unescorted physical access to CCAs. RFC_URE1 identified the cause of this violation as failure to integrate its list of individuals with access to CCAs with its rosters of those individuals requiring CIP training.	CIP-004-1	R2; R2.1.3; R2.3.	Lower	Lower	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. All individuals involved in the violation of CIP-004-1 R2 had successfully completed personnel risk assessments (PRAs) that revealed no criminal history or other identity issues that would have prevented them from receiving CIP qualifications prior to RFC_URE1 granting the individuals at issue access to Critical Cyber Assets (CCAs). Further, all individuals involved in the violation received either CIP training or corporate cyber awareness training in advance of RFC_URE1 granting them access to CCAs. While six of those individuals had not received any of the required CIP training, they did receive corporate cyber awareness training. RFC_URE1's corporate cyber awareness training, while not a substitute for formal CIP training, includes basic information on cyber risks. Additionally, of the 183 individuals who did not receive annual training pursuant to CIP-004-1 R2.3, 54 of the individuals with cyber access had read-only access and could not effect a change in the Energy Management System. The remaining 15 individuals with cyber access had all completed initial CIP training, but did not undergo timely annual training. The remaining 122 individuals with physical access who had not received annual training pursuant to CIP-004-1 R2.3 all had previously completed either CIP training or RFC_URE1's corporate cyber awareness training. Of the total employees and contractors with access to RFC_URE1 CCAs, less than 5% were involved in the violation of CIP-004-1 R2.1. The violation of CIP-004-1 R2.3 involved less than 5% of the total training sessions RFC_URE1 has administered in a 34-month period.	Effective date of the Standard	Mitigation Plan completion
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000662	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a possible violation of CIP-004-1 R3. Reliability*First* determined that RFC_URE1 violated CIP-004-1 R3 when it did not perform initial personnel risk assessments (PRAs) or updated PRAs for a total of 109 individuals with cyber or unescorted physical access to Critical Cyber Assets (CCAs). RFC_URE1 discovered that 109 individuals did not undergo an initial PRA or receive an updated PRA, as required by CIP-004-1 R3 and CIP-004-1 R3.2. Specifically, RFC_URE1 determined that 107 individuals did not have an initial PRA within 30 days from the date RFC_URE1 granted them access to CCAs, as required by CIP-004-1 R3. Out of the 107 individuals: 52 were RFC_URE1 employees with cyber access to CCAs; 38 were RFC_URE1 employees with unescorted physical access to CCAs; and 17 were contractors with physical access to CCAs. Of the 52 individuals with cyber access, none had cyber access to CCAs located at the system control center. Three of the individuals with physical access had access to CCAs located at the system control center. Additionally, RFC_URE1 did not perform an updated PRA for two RFC_URE1 employees within seven years of their previous PRAs as required by CIP-004-1 R3.2. RFC_URE1 previously granted these two employees unescorted physical access to CCAs. RFC_URE1 identified the cause of this violation as insufficient monitoring of the process for updating PRAs and incomplete PRA document maintenance. RFC_URE1 noted that it granted 100 of the 109 individuals at issue access to CCAs prior to CIP-004-1 R2's mandatory compliance date and identified this as a contributing factor to this violation.	CIP-004-1	R3; R3.2	Medium	High	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. The 52 individuals with cyber access and missing PRAs had read-only access and could not effect a change to the Energy Management System. Additionally, the location to which 57 of the individuals had unescorted physical access is staffed and monitored 24 hours a day, seven days a week. In addition, the location has procedural controls for monitoring physical access at all access points that uniquely identifies the individuals involved and records when the individuals accessed the location.	Effective date of the Standard	Mitigation Plan completion

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201000306	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a possible violation of CIP-004-1 R4. Reliability*First* determined that RFC_URE1 violated the Standard by not maintaining its Critical Cyber Assets (CCAs) access list, not reviewing its CCA access list on a quarterly basis beginning on the effective compliance date, and not removing 67 individuals who no longer required access to the CCAs from its CCA access lists within the required timeframes. This violation includes three separate issues, all of which of involved CIP-004-1 R4. First, during a quarterly review conducted for the period 18 months after the effective compliance enforcement date, RFC_URE1 determined that 105 individuals (85 RFC_URE1 employees and 20 contractors) had unescorted physical access to CCAs without evidence that RFC_URE1 had granted them access at a prior date. None of the 105 individuals had physical access to CCAs located at the system control center. This quarterly review was the first during which RFC_URE1 compared its paper-based CCA access list to its database access list. RFC_URE1 could not locate original documentation from its paper-based process to demonstrate it previously granted physical access to the 105 individuals. Therefore, RFC_URE1 did not maintain a list of authorized personnel, as required by CIP-004-1 R4. Second, RFC_URE1 did not perform reviews of its physical access lists for CCAs during the required first twelve months of mandatory compliance. Pursuant to the CIP Implementation Plan promulgated by NERC, RFC_URE1 was not required to implement CIP-006-1, which requires RFC_URE1 to create and maintain a physical security plan for access points to CCA, until a year after the effective compliance date of CIP-004-1. RFC_URE1 incorrectly concluded, based on its understanding of CIP-006-1, that it therefore did not have to conduct quarterly reviews of its access lists pursuant to CIP-004-1 R4.1 until CIP-006-1's effective compliance date; however, RFC_URE1 was required to review its physical access lists on a quarterly basis beginning one year prior, and therefore did not comply with CIP-004-1 R4.1. Finally, RFC_URE1 discovered that for a 22-month period, it did not revoke cyber or physical access to CCAs for 67 individuals within the required timeframe pursuant to CIP-004-1 R4.1 and R4.2. Specifically, 55 of the 67 individuals resigned but RFC_URE1 did not revoke their access within seven calendar days. Also, RFC_URE1 transferred nine of the 67 individuals to positions that did not require access to CCAs but did not revoke their access within seven calendar days. The remaining three individuals were terminated for cause, but RFC_URE1 did not revoke their access to CCAs within 24 hours, as required by CIP-004-1 R4.2. Regarding the third issue, 41 occurrences involved resignation or transfers for which RFC_URE1 cannot locate any documented evidence that it revoked access. Seventeen occurrences involved an RFC_URE1 supervisor who did not notify appropriate staff within seven days that the individuals no longer needed access to the CCAs. Six occurrences involved human error in which RFC_URE1 staff did not notify necessary personnel of a revocation within the seven day time period. As to the individuals terminated for cause, RFC_URE1 personnel did not notify appropriate staff necessary to effectuate revocation of these individuals' access within the required 24-hour timeframe. The employees terminated for cause remained on the access list 81, 20 and 70 days in excess of the 24-hour timeframe, respectively.	CIP-004-1	R4; R4.1; R4.2	Medium	Severe	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. RFC_URE1 performed CIP training and personnel risk assessments (PRAs) for the 105 individuals with access to RFC_URE1's CCAs, but for whom RFC_URE1 could not produce evidence of authorized access. Additionally, for the instances where RFC_URE1 did not revoke CCA access from individuals who resigned, were transferred, or terminated for cause, RFC_URE1 confirmed that 64 of the 67 individuals did not access the CCAs beyond the prescribed time period. In the three instances in which individuals may have accessed CCAs, the individuals had read-only access and therefore could not modify any CCAs. These individuals were not the same three individuals that were terminated for cause. These three individuals were transferred or rehired and remain employees of RFC_URE1.	Effective date of the Standard	Date RFC_URE1 revoked access rights to CCAs for individuals who had either resigned, were transferred, or were terminated for cause and had incorrectly remained on RFC_URE1's access list
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100774	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a possible violation of CIP-007-2 R4. Reliability*First* determined that RFC_URE1 was in violation of the Standard for failing to use anti-virus software and other malware prevention tools or implement and document compensating measures on three Critical Cyber Assets (CCAs) within its Electronic Security Perimeter in violation of CIP-007-2 R4. RFC_URE1 discovered it was not using anti-virus software and other malware prevention tools on three CCAs pursuant to CIP-007-2 R4. None of the three CCAs had an ability to control bulk power system (BPS) facilities. The CCAs were incapable of using anti-virus software and other malware prevention tools, but RFC_URE1 never submitted a Technical Feasibility Exception (TFE) request to Reliability*First* for the three CCAs at issue. RFC_URE1 incorrectly categorized one CCA on the RFC_URE1 CCA list as a server, rather than an appliance based on an operating system. Due to this error, RFC_URE1 did not create a TFE request for this CCA. RFC_URE1 did not submit TFE requests for the remaining two CCAs because it did not account for the two CCAs while reviewing its CCA list. Reliability*First* determined that RFC_URE1 did not use anti-virus software and other malware prevention tools or implement and document compensating measures on three CCAs within its Electronic Security Perimeter in violation of CIP-007-2 R4.	CIP-007-2	R4	Medium	Severe	This violation posed a moderate risk to the reliability of the BPS because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. RFC_URE1 kept all three CCAs in physically protected locations at all times during the duration of the violation. Also, although it was technically infeasible for RFC_URE1 to employ malware prevention tools on the CCAs, RFC_URE1 did have multiple layers of defenses in place during the duration of the violation to reduce the CCA's risk of exposure to malware. These included, but were not limited to: perimeter defenses such as firewalls and logging; network defenses such as intrusion detection and prevention software; host defenses such as firewalls and malware on other assets; and procedural controls such as cyber policies and procedures.	Deadline for submitting timely TFEs for the three CCAs at issue	Date RFC_URE1 removed the last of the three CCAs from its system
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100775	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a possible violation of CIP-007-2 R5.3. This Self-Report identified two separate issues, both of which involved CIP-007-2 R5.3. Reliability*First* determined that RFC_URE1 was in violation of the Standard as it did not use, and change within the required timeframe, passwords that met the specifications of CIP-007-2 R5.3. First, RFC_URE1 determined three Critical Cyber Assets (CCAs), although capable of processing passwords, were incapable of processing complex passwords such as those required by CIP 007-2 R5.3.1 and R5.3.2. The three CCAs at issue in this violation are the same CCAs associated with the CIP-007-2 R4.1 violation. RFC_URE1 never submitted TFE requests for the three CCAs at issue. Second, RFC_URE1 did not update 91 shared account passwords associated with the three CCAs at issue within the annual timeframe as required by CIP-007-2 R5.3.3. RFC_URE1 did not change the passwords due to insufficient controls to validate that it changed all shared account passwords annually.	CIP-007-2	R5; R5.3	Lower	Severe	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. RFC_URE1 kept all three CCAs in physically protected locations at all times during the duration of the violation. Also, although it was technically infeasible for RFC_URE1 to require and use passwords subject to the requirements found in CIP-007-2 R5.3's sub-requirements for the three CCAs, RFC_URE1 had multiple layers of defenses in place to protect the CCAs during the duration of the violation. These defenses included, but were not limited to: perimeter defenses such as firewalls and logging; network defenses such as intrusion detection and prevention software; host defenses such as firewalls and malware on other assets; and procedural controls such as cyber policies and procedures.	Deadline for submitting timely TFEs for the three CCAs at issue	Date RFC_URE1 removed the last of the three CCAs from its system
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 1 (RFC_URE1)	NCRXXXXX	RFC201100999	Settlement Agreement	RFC_URE1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-007-3 R6. During a review of historical logs, RFC_URE1 discovered that it was missing the log records for a 41-day period for one Cyber Asset within its Electronic Security Perimeter (ESP). The Cyber Asset at issue is installed on host servers that are Critical Cyber Assets (CCAs) and part of the Energy Management System. The Cyber Asset allows multiple operating systems to function concurrently on the host servers. The violation was caused by an error-handling routine that created a number of log files, but which eliminated the oldest logs, some of which were less than 90 days old. Reliability*First* determined RFC_URE1 violated the Standard by failing to retain the logs specific to the Cyber Asset within its ESP for ninety calendar days pursuant to CIP-007-3 R6.4. Further, Reliability*First* determined that because RFC_URE1 could not locate the logs for one Cyber Asset within its ESP, it was incapable of reviewing all the logs of system events related to cyber security and therefore did not comply with CIP-007-3 R6.5.	CIP-007-3	R6; R6.4; R6.5	Lower	Severe	This violation posed a moderate risk to the reliability of the bulk power system (BPS) because of the nature of the violation, offset by the mitigating factors. This violation did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by the following factors. The Cyber Asset at issue is physically located within PSPs. Further, the purpose of the Cyber Asset is to manage operating systems within a host server and as such, the Cyber Asset provides no ability to control BPS facilities.	First date which RFC_URE1 did not have historical logs for the Cyber Asset at issue	Last date for which RFC_URE1 was missing historical logs for the Cyber Asset at issue

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC201000646	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst identifying a possible violation of CIP-004-1 R4. During a quarterly review, RFC_URE2 determined that unescorted physical access to its system given to some personnel was not documented, in violation of the Standard. The group consisted of 64 individuals - 60 employees and 4 contractors. RFC_URE2 conducted quarterly reviews; however, this quarterly review was the first during which RFC_URE2 compared its paper-based CCA access list to its CIP access database system. RFC_URE2 could not locate evidence for the 64 individuals through its paper-based process or in its CIP access database system access list to demonstrate that RFC_URE2 previously authorized physical access to the 64 individuals at issue. ReliabilityFirst determined that RFC_URE2 violated CIP-004-1 R4 for failing to maintain its CCA access list for 64 individuals.	CIP-004-1	R4	Lower	Lower	ReliabilityFirst determined that this violation posed a moderate and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the is a collection of Critical Cyber Assets (CCAs) with the ability to monitor the parent company's power plants allowing for limited control over power levels. At no time did any unqualified, unauthorized individuals have the ability to use the system to monitor or control any of the parent company's power plants. Of the 64 individuals at issue in this violation, 54 had no logical access to the system. The remaining ten individuals were qualified for logical access to the system. RFC_URE2 granted these ten individuals authorized cyber access to the system prior to the violation. All 64 individuals that had unescorted physical access completed CIP training prior to the violation. Additionally, RFC_URE2 conducted personnel risk assessments (PRAs) for 63 of the 64 of the individuals prior to the violation. None of the PRAs revealed any criminal history or other identity issues that would have prevented the employees' CIP qualification. The PRA for the employee who did not have one performed prior to the violation revealed no criminal history or other identity issues that would have prevented the employee's CIP qualification.	When Standard became mandatory and enforceable	When RFC_URE2 either revoked physical access or properly granted unescorted physical access rights to its CCAs for each of the 64 individuals at issue
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 2 (RFC_URE2)	NCRXXXXX	RFC2011001073	Settlement Agreement	RFC_URE2 submitted a Self-Report to ReliabilityFirst in its response to a Request for Information issued by ReliabilityFirst in relation to a violation of CIP-004-1 R4. RFC_URE2 could not provide evidence that it conducted a Personnel Risk Assessment (PRA) for one employee within thirty days of that employee having physical access to Critical Cyber Assets (CCAs). ReliabilityFirst determined that RFC_URE2 violated CIP-004-1 R3 when it could not provide evidence it conducted a PRA for an employee within thirty days of that employee having physical access to CCAs.	CIP-004-1	R3	Medium	High	ReliabilityFirst determined that this violation posed a moderate and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the system is a collection of Critical Cyber Assets (CCAs) with the ability to monitor the parent company's power plants allowing for limited control over power levels. Further, RFC_URE2 did not report this alleged violation as part of its initial self report. Rather, RFC_URE2 discovered the violation several months later while compiling responses to a formal Request for Information from ReliabilityFirst concerning the self reported violation of CIP-004. At no time did any unqualified, unauthorized individuals have the ability to use the system to monitor or control any of the parent company's power plants. The employee completed CIP training prior to the violation. Further, RFC_URE2 removed the employee's physical access rights. Also, when RFC_URE2 conducted a PRA for the employee, it revealed no criminal history or other identity issues that would have prevented the employee's CIP qualification. Finally, RFC_URE2 examined the access logs and determined that although the employee had unescorted physical access rights, the employee did not actually access any RFC_URE2 physical security perimeters during the duration of the violation.	When Standard became mandatory and enforceable	When RFC_URE2 removed the employee's physical access rights to CCAs
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3) RFC_URE3a, RFC_URE3b and RFC_URE3c are subsidiaries of a single parent company, collectively known as the RFC_UREs	NCRXXXXX	RFC201000440	Settlement Agreement	The RFC_UREs submitted Self-Reports to ReliabilityFirst identifying possible violations of CIP-004-1 R4. During an internal audit, the RFC_UREs discovered that they failed to review their access lists of personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) quarterly, in violation of CIP-004-1 R4.1. The RFC_UREs failed to revoke authorized cyber or authorized unescorted physical access to CCAs for 23 individuals in a timely manner, a violation of CIP-004-1 R.4.2. As a result, the RFC_UREs failed to timely update the access lists within seven calendar days to reflect these access right changes, a violation of CIP-004-1 R4.1. Specifically, RFC_URE3a failed to revoke the access of five individuals who no longer required such access within seven calendar days. The CCAs at issue at RFC_URE3a were transmission assets.	CIP-004-1	R4; R4.1; R4.2	Lower	High	ReliabilityFirst determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all physical access locations are controlled areas requiring card key access and are staffed or monitored using alarm systems and video at all times. All individuals at issue in the violations received the requisite personnel risk assessments and NERC CIP training. In addition, all RFC_URE3a individuals were transferred within the RFC_UREs and were employees in good standing at the time. Lastly, for all individuals whose access was not timely revoked, there were no attempts to access CCAs prior to the revocation of access.	Date access should have been revoked in first instance	Date access was revoked and interim process for access review implemented
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3) RFC_URE3a, RFC_URE3b and RFC_URE3c are subsidiaries of a single parent company, collectively known as the RFC_UREs	NCRXXXXX	RFC201000441	Settlement Agreement	The RFC_UREs submitted Self-Reports to ReliabilityFirst identifying possible violations of CIP-004-1 R4. During an internal audit, the RFC_UREs discovered that they failed to review their access lists of personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) quarterly, in violation of CIP-004-1 R4.1. The RFC_UREs failed to revoke authorized cyber or authorized unescorted physical access to CCAs for 23 individuals in a timely manner, a violation of CIP-004-1 R.4.2. As a result, the RFC_UREs failed to timely update the access lists within seven calendar days to reflect these access right changes, a violation of CIP-004-1 R4.1. Specifically, RFC_URE3b failed to revoke the access of seven individuals who no longer required such access within seven calendar days. The CCAs at issue at RFC_URE3b were transmission assets.	CIP-004-1	R4; R4.1; R4.2	Lower	High	ReliabilityFirst determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all physical access locations are controlled areas requiring card key access and are staffed or monitored using alarm systems and video at all times. All individuals at issue in the violations received the requisite personnel risk assessments and NERC CIP training. In addition, only one of the RFC_URE3b individuals was terminated (not for cause); all remaining individuals were transferred within the RFC_UREs and were employees in good standing at the time. The terminated individual's employee badge key card used for physical access was confiscated and disabled along with the employee's computer network logins upon termination. Lastly, for all individuals whose access was not timely revoked, there were no attempts to access CCAs prior to the revocation of access.	Date access should have been revoked	Date access was revoked and interim process for access review implemented

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Reliability*First* Corporation (Reliability*First*)	Unidentified Registered Entity 3 (RFC_URE3) RFC_URE3a, RFC_URE3b and RFC_URE3c are subsidiaries of a single parent company, collectively known as the RFC_UREs	NCRXXXXX	RFC201000442	Settlement Agreement	The RFC_UREs submitted Self-Reports to ReliabilityFirst identifying possible violations of CIP-004-1 R4. During an internal audit, the RFC_UREs discovered that they failed to review their access lists of personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) quarterly, in violation of CIP-004-1 R4.1. The RFC_UREs failed to revoke authorized cyber or authorized unescorted physical access to CCAs for 23 individuals in a timely manner, a violation of CIP-004-1 R.4.2. As a result, the RFC_UREs failed to timely update the access lists within seven calendar days to reflect these access right changes, a violation of CIP-004-1 R4.1. Specifically, RFC_URE3c failed to revoke the access of eleven individuals who no longer required such access within seven calendar days. The CCAs at issue at RFC_URE3c were generation assets.	CIP-004-1	R4; R4.1; R4.2	Lower	High	ReliabilityFirst determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all physical access locations are controlled areas requiring card key access and are staffed or monitored using alarm systems and video at all times. All individuals at issue in the violations received the requisite personnel risk assessments and NERC CIP training. In addition, all RFC_URE3c individuals were transferred within the Exelon Companies and were employees in good standing at the time. Lastly, for all individuals whose access was not timely revoked, there were no attempts to access CCAs prior to the revocation of access.	Date access should have been revoked	Date access was revoked and interim process for access review implemented
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000136	Settlement Agreement	Six months after the mandatory compliance enforcement date, Texas RE_URE1 determined that it did not make its cyber security policy readily available to contractors with access to, or responsibility for, Critical Cyber Assets (CCAs) in another reliability region. As a result of an extended investigation, Texas RE_URE1 determined that the same issue existed in the Texas RE region and self-reported a violation of CIP-003-1 R1. The cyber security policy was not made available to contractors, which make up 6.7 percent of employees. None of the contractors were actually responsible for CCAs. The policy was readily available to the remaining 93.3 percent of permanent employees.	CIP-003-1	R1; R1.2	Lower	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS). The violation did not pose a serious or substantial risk to the BPS because Texas RE_URE1 failed to make the cyber security policy available to only a small percentage (6.7%) of employees (all the contractors). The policy was readily available to permanent employees. Second, there were no compromises, or attempts to compromise, the Electronic Security Perimeter or Physical Security Perimeter of a CCA during the period of the violation. Further, there were no disruptions or attempts to disrupt the operation of a CCA during the period of the violation.	The date the requirement became enforceable for the entity	Mitigation Plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201002604	Settlement Agreement	WECC_URE1 self-reported a violation of regional standard BAL-004-WECC-01 R4.4. WECC_URE1 stated that it failed to synchronize its Time Error to the nearest 0.001 seconds of the System Time Error by comparing its reading to the reading broadcast by the Interconnection Time Monitor. WECC_URE1 failed to inform its Energy Management System (EMS) personnel of the requirement to obtain this daily time error value. Also, WECC_URE1 failed to synchronize its time error daily value with the value issued by the WECC Reliability Coordinator (WECC RC). In response to a WECC information request, WECC_URE1 stated that the lapse was due to internal communication error and the notification was misplaced. WECC_URE1's support staff became aware of the issue and immediately implemented the daily synchronization. Based on the record, WECC determined that WECC_URE1 failed to synchronize its time error, in violation of this Standard.	BAL-004-WECC-01	R4.4	Lower	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 although WECC_URE1 failed to synchronize its daily Time Error with the WECC RC, it did compute its hourly Primary Inadvertent Interchange value, which is used to calculate the Automatic Time Error Correction and maintain the reliability of the BPS. Also, because the hourly time error was synchronized, WECC_URE1's failure to synchronize daily the Time Error value did not affect the scheduled flow of energy needed in real time to support demand, and therefore posed a minimal risk to the reliability of the BPS.	The date WECC_URE1 was required to comply with this Standard	When WECC_URE1 began performing the required daily Time Error checks
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102807	Settlement Agreement	WECC_URE1 submitted a Self-Report for noncompliance with CIP-004-1 R2, stating that in preparation of its Audit, it discovered some discrepancies in its training records. WECC_URE1 failed to ensure that all personnel having access to Critical Cyber Assets (CCAs), including contractors and vendors, are trained prior to being granted such access, except in specified circumstances such as an emergency. Also, WECC_URE1 failed to maintain documentation that training is conducted at least annually, and did not keep a record of the date training was completed and a record of attendance. WECC determined that one individual did not receive training prior to receiving access to the CCAs and four employees did not receive annual training. Based on the record, WECC determined that WECC_URE1 violated CIP-004-1 R2.1 for failure to ensure that all individuals with access to the CCAs are trained prior to being granted such access, and violated CIP-004-1 R2.3 for failure to maintain documentation that training was completed at least annually.	CIP-004-1	R2.1/ R2.3	Lower	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 although WECC_URE1 failed to ensure proper training and maintain documentation related to employee training, the individuals in scope had current Personnel Risk Assessments (PRAs) and their electronic access was read-only. Also, the individuals had access to six Physical Security Perimeters (PSPs) and one Electronic Security Perimeter (ESP) which contain CCAs, but the PSPs and the ESP have logging and monitoring systems in place. Therefore, WECC determined that this violation had a minimal impact on the reliability of the BPS.	When WECC_URE1 failed to implement its annual training program	When WECC_URE1 completed its Mitigation Plan

Nextera Energy Resources, LLC

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC20100599	Settlement Agreement	WECC notified WECC_URE1 that WECC was initiating the semi-annual Self-Certification process. WECC_URE1 submitted a Self-Certification. WECC_URE1 self-reported a violation of CIP-006-1 R1, stating that it failed to ensure Cyber Assets used in the Access Control and Monitoring (ACM) of the Physical Security Perimeters (PSPs) were afforded all the protections specified in CIP-006-1 R1.8. WECC performed an on-site Audit, which included compliance with CIP-006-1 R1.8, and determined that WECC_URE1 failed to ensure that Cyber Assets used in the ACM of the PSPs were afforded the protective measures specified in CIP-005 R3 (WECC_URE1 has five switches which are electronic access points to seven physical ACM controllers, these switches were not configured to send syslogs to the WECC_URE1's syslog server; therefore, alerts generated from these controllers were not able to appropriately notify designated personnel), CIP-007 R3 (WECC_URE1 failed to document an assessment for applicability of security patches within 30 days of the patch being made available for three physical ACM devices and WECC_URE1 failed to document an assessment of security patches for sixteen Cyber Assets (switches) located in the Electronic Security Perimeters (ESPs) and for five devices used in the access control and monitoring of the ESPs), and CIP-009 R4 and R5 (WECC_URE1 failed to include the backup and restore procedures for seven physical ACM control panels in its Recovery Plan, which are used to store access control authentication data for the card readers and WECC_URE1 failed to follow its documented procedure of documenting annual testing of information essential to recovery that is stored on backup media; specifically, testing was done but documentation was not completed to demonstrate compliance), in violation of CIP-006-1 R1.8.	CIP-006-1 (the violation involves later versions of this standard--CIP-006-2 R2.2 and CIP-006-3 R2.2)	R1.8	Lower	Severe	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 there were several compensating measures in place to mitigate the risk. First, WECC_URE1 stated that only personnel with current training and Personnel Risk Assessments (PRAs) had access to the devices in question. Also, WECC_URE1's server was equipped with anti-virus and malware protection tools, and was also located within a Physical Security Perimeter (PSP) and secured by a firewall. The seven controllers associated with noncompliance with CIP-009 R4 were located in physically secured rooms.	The date WECC_URE1 was required to comply with this Standard	When WECC_URE1 mitigated its violation
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102609	Settlement Agreement	WECC_URE1 submitted a Self-Certification stating that it failed to document the assessment of thirteen security patches and security upgrades for applicability within 30 calendar days of availability of the patches or upgrades. Based on the record, WECC determined that WECC_URE1 failed to assess security patches for 21 Cyber Assets, which resulted in WECC_URE1's failure to make sufficient records of its security patch management program, in violation of CIP-007-1 R3.1.	CIP-007-1	R3.1	Lower	Severe	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 the risk was mitigated by the fact that the devices in scope are located in a Physical Security Perimeter (PSP) and Electronic Security Perimeter (ESP) and thus afforded the protections specified in CIP-005 and CIP-006, including automated security status monitoring.	The date WECC_URE1 was required to comply with this Standard	When WECC_URE1 completed its Mitigation Plan
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC201102606	Settlement Agreement	WECC_URE1 submitted a Self-Report for a violation of CIP-007-1 R6. WECC_URE1 stated that it failed to implement monitoring and logging for two new Cyber Assets and failed to document the process for monitoring and logging for eight existing Cyber Assets located in its Generation Management System (GMS) Electronic Security Perimeter (ESP). WECC determined that WECC_URE1 failed to implement and document the organizational process and technical and procedural mechanisms for monitoring of security events on all Cyber Assets within the ESP, in violation of CIP-007-1 R6.	CIP-007-1	R6	Lower	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 the risk was mitigated by the fact that the devices in scope were not classified as Critical Cyber Assets (CCAs). Also, the Cyber Assets were afforded the physical protection required by CIP-006 and did not have remote access.	The date WECC_URE1 was required to comply with this Standard	When WECC_URE1 completed its Mitigation Plan
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC20112613	Settlement Agreement	WECC_URE1 submitted a Self-Certification stating that it failed to perform annually an assessment on its system for the time period. WECC_URE1 last performed an assessment in the fall of the prior year and again in the winter of the next year. WECC_URE1's system contains 12 Cyber Assets. Based on the record, WECC determined that WECC_URE1 failed to perform an annual assessment on 12 Cyber Assets, in violation of CIP-007-3 R8.	CIP-007-3	R8	Lower	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 the risk was mitigated by the fact that the devices in scope were located in a Physical Security Perimeter (PSP) and an Electronic Security Perimeter (ESP) and thus were afforded the protections listed in CIP-005 and CIP-006. In addition, all individuals with access to the devices had completed training and Personnel Risk Assessments (PRAs), thus minimizing the risk to the BPS.	When WECC_URE1 failed to perform annual assessment	When WECC_URE1 completed its Mitigation Plan

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 1 (WECC_URE1)	NCRXXXXX	WECC200901475	Settlement Agreement	WECC_URE1 submitted five Self-Reports for noncompliance with this Standard in the period for approximately six months. Based on the record, WECC determined that the first Self-Report identified the initial instance of noncompliance and the subsequent Self-Reports expanded the scope of the initial Self-Report. In its first Self-Report, WECC_URE1 stated that after upgrading its e-tagging applications, it experienced intermittent database deadlocks that interfered with normal operations. WECC_URE1 failed to respond to numerous e-tag requests requiring WECC_URE1's approval from the Interchange Authority to transition Arranged Interchanges to Confirmed Interchanges, and as a result the e-tags expired. WECC reviewed all five reports and determined that WECC_URE1 failed to respond to more than 50 e-tag requests identified in each Self-Report.	INT-006-2	R1	Lower	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 although WECC_URE1 failed to respond to 63 e-tags, it responded to the majority of requests from Interchange Authorities within the requisite timeframe during the violation period. Also, WECC_URE1 has the ability to process expired tags through direct contact with the appropriate entities. Finally, WECC determined that when the more than 50 expired e-tags are considered in the context of the total number of e-tags coordinated by WECC_URE1, the risk to the BPS from non-compliance is reduced.	When WECC_URE1 failed to respond before tags expired	When WECC_URE1 completed its Mitigation Plan
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002246	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). During the Audit, WECC found that for 20 minutes, on a single day, WECC_URE2 operated in an Automatic Generation Control (AGC) mode other than the Automatic Time Error Correction (ATEC) and failed to notify all other Balancing Authorities (BAs) of its operating mode. Specifically, the WECC Audit team (Audit Team) determined that WECC_URE2 operated with its ATEC out of service from 12:44 to 13:04 when it switched to its Tie Line Bias (TLB) AGC mode. WECC_URE2 dispatcher logs reflect that at 12:40 pm the dispatcher changed WECC_URE2's AGC mode from ATEC to its TLB AGC because the ATEC was sending incorrect values to one of WECC_URE2's neighboring BAs. The dispatcher logs further reflect that at 13:04, the ATEC problem was resolved. WECC_URE2 could not provide evidence that it notified other BAs when it operated its AGC in a mode other than ATEC from 12:44 through 13:04. WECC determined that WECC_URE2 was in violation of BAL-004-WECC-01 R2 for failing to notify its BAs when it operated its AGC system in a mode other than ATEC.	BAL-004-WECC-01	R2	Lower	Lower	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) due to the limited duration (20 minutes) WECC_URE2 was operating in an AGC mode other than ATEC. In addition, WECC_URE2 created an alarm for the AGC so that when the AGC system is functioning in any mode except ATEC mode, an alarm is generated to send WECC a message immediately. WECC RC's messaging system, in turn, automatically retransmits the message to its subscribers which include the region's BAs. This alarm will prevent future instances of failing to notify the BA.	Date WECC_URE2 operated its AGC in a mode other than ATEC without notifying its BAs	Date WECC_URE2 operated its AGC in a mode other than ATEC without notifying its BAs
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002391	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). As a part of the Audit, the WECC Audit team (Audit Team) requested from WECC_URE2 documentation of its cyber security policy, in compliance with CIP-003-1 R1. According to the Audit Team, WECC_URE2 provided three different versions of its cyber security policy. After reviewing all three versions of WECC_URE2's cyber security policy, the Audit Team concluded that WECC_URE2's first two versions of WECC_URE2's cyber security policy violated the Standard because they addressed CIP-002 through CIP-009 in a general manner, as opposed to a more specific directive tailored to how the entity's management intend that the organization will go about addressing each requirement individually. WECC determined that WECC_URE2 was in violation of CIP-003-1 R1 because its cyber security policy did not sufficiently address the requirements of CIP-002 through CIP-009. Specifically, WECC_URE2's cyber security policy addressed the requirements of CIP-002 through CIP-009 too broadly and should have addressed those requirements in more detail in compliance with the Standard.	CIP-003-1	R1	Medium	Severe	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). Although an insufficient cyber security policy would have resulted in WECC_URE2 personnel not having proper direction and guidance in the proper handling of Critical Cyber Assets (CCAs), causing a lack of understanding or the unavailability of CCAs, WECC_URE2 did have some documentation of a cyber security policy that addressed the requirements of CIP-002 through CIP-009, though not in specific detail. In addition, WECC_URE2 developed a detailed cyber security policy prior to the Audit to address the requirements of the Standard.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002393	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit), including CIP-003-1 R6. As a part of the Audit, the WECC Audit team (Audit Team) requested from WECC_URE2 documentation that it had a change control and configuration management program, in compliance with CIP-003-1 R6. WECC_URE2 provided three procedure documents. Upon review of these documents, WECC determined that these documents did not include processes for configuration management and thus, WECC_URE2 was in violation of the Standard.	CIP-003-1	R6	Lower	Lower	WECC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the bulk power system (BPS). Configuration management is essential to controlling system changes. It is possible that if a change to the system is improperly configured due to the lack of configuration management, the improperly configured change can negatively impact other parts of the system. However, the CCAs in question were located inside Electronic Security Perimeters and Physical Security Perimeters and afforded some of the protections of CIP-005-1 R1 and CIP-006- R1.	When the Standard became mandatory and enforceable for WECC_URE2	Date WECC_URE2 documented a process for configuration management

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002296	Settlement Agreement	WECC_URE2 self-reported potential noncompliance with CIP-004-1 R2.3. 4.5 months later, a WECC subject matter expert (SME) held a conference call with WECC_URE2 to discuss the violation. On the call the WECC SME confirmed the information contained in WECC_URE2's Self-Report that WECC_URE2 identified an employee who had exceeded his annual training date requirement. Subsequently, WECC_URE2 conducted an internal review and identified three additional employees who had exceeded their training renewal dates. These individuals were due for training 40 days before the discovery date. WECC_URE2 stated in its Self-Report that the personnel identified as having exceeded their training dates had been trained within fourteen months, their access rights to Critical Cyber Assets (CCAs) were immediately revoked and, once the personnel had been properly trained, their access to CCAs were reinstated. WECC determined that WECC_URE2 was in violation of CIP-004-1 R2.3 because it failed to maintain an annual cyber security training program and allowed the training of four of its employees with access to CCAs to lapse.	CIP-004-1	R2; R2.3	Lower	High	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the violation was limited to only four individuals, and those few individuals only missed their training dates by two months. Although this lack in proper training could have led to mismanagement of CCAs and reduced reliability to the BPS, this risk was mitigated by the fact these individuals had previous training and previous authorized access to the CCAs.	When the Standard became mandatory and enforceable for WECC_URE2	When WECC_URE2 revoked access to CCAs for the affected personnel
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002394	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). During the Audit, WECC found that WECC_URE2 maintained a list of all personnel with unescorted physical cyber access to Critical Cyber Assets (CCAs) and reviewed the access on a quarterly basis; however, the quarterly reviews did not include its personnel's specific electronic access rights to CCAs. WECC determined that WECC_URE2 was in violation of the Standard for not including electronic access rights in its quarterly reviews of personnel who have unescorted access to CCAs.	CIP-004-1	R4	Lower	Moderate	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). Although it was possible that because WECC_URE2 did not review electronic access right in its quarterly reviews of personnel with unescorted access to CCAs, unauthorized personnel could have gained electronic access to CCAs and acted maliciously, WECC_URE2 did have compensating measures in place. WECC_URE2 did perform quarterly reviews of its personnel assigned to particular job functions, and WECC_URE2's electronic access rights were tied to specific job functions. While this review of job functions was not a sufficient review to make it compliant with CIP-004-1 R4, it functioned as an indirect review of specific electronic access rights.	When the Standard became mandatory and enforceable for WECC_URE2	When WECC_URE2 mitigated the violation
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002399	Settlement Agreement	WECC_URE2 self-reported a potential violation CIP-005-1 R1.5. In its Self-Report, WECC_URE2 stated that it had test procedures in place to test security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms or other third-party software or firmware before placing software or firmware into production on Cyber Assets. WECC_URE2 also stated in the Self-Report that, based on a misinterpretation of CIP-007-1 R1, WECC_URE2 did not specifically test software and firmware to determine if it would have adverse affects on existing cyber security controls. In addition, WECC_URE2 self-reported that it has a patch management program in place to evaluate, test, and install applicable security patches for all Cyber Assets inside its Electronic Security Perimeter, but the program is focused on operating system and major application patches, and minor or peripheral applications were not addressed consistently. Seven months after self-reporting, WECC_URE2 submitted additional evidence identifying specifically the Cyber Assets that were not afforded the protections in CIP-007-1 R1 and R3. WECC determined that WECC_URE2 was in violation of the Standard because it did not afford its Cyber Assets used in the access control and monitoring of its Electronic Security Perimeter the protections in CIP-007-1 R1 and R3. Specifically, WECC_URE2 was in violation of CIP-005-1 R1.5 because it did not test its Cyber Assets to ensure that new Cyber Assets and significant changes to Cyber Assets would not adversely affect existing cyber security controls. Additionally, WECC_URE2 did not evaluate, test and install applicable security patches for all Cyber Assets as prescribed by CIP-007-1 R3.	CIP-005-1	R1; R1.5	Lower	Moderate	WECC determined that this violation posed a moderate and not a serious or substantial risk to the bulk power system (BPS). The purpose of this Standard is to identify and protect the Electronic Security Perimeter by protecting all access points on the perimeter. Failure to ensure that Cyber Assets used in the access control and/or monitoring (ACM) of the Electronic Security Perimeter have the appropriate protective measures as specified in CIP-007-1 R1 and R3 may allow unauthorized internal and or external access to these Cyber Assets, which could then allow for successful cyber attacks against Critical Cyber Assets essential for operation of the BPS thereby negatively impacting the operation of the BPS. In this instance, WECC_URE2 failed to ensure that new and changes to Cyber Assets would not have a negative impact on the existing cyber controls and also failed to evaluate, test, and install security patches for all Cyber Assets. However, the Cyber Assets were afforded all the remaining protection required by CIP-005-1 R1.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002397	Settlement Agreement	WECC_URE2 self-reported a potential violation CIP-006-1 R1. In its Self-Report, WECC_URE2 stated that it has not created or implemented cyber security test procedures for its physical access control that are performed in a manner that reflects its production environment. In addition, because these tests have not been performed, they have not been documented. WECC_URE2 further self-reported that it was in violation of CIP-006-2 R2.2 because its physical access control systems run on one type of operating systems and WECC_URE2's program for security patch management has not been formally documented and does not appear to comply strictly with what is called for in requirement CIP-006-2 R2.2. Seven months after self-reporting, WECC_URE2 submitted additional evidence identifying specifically the Cyber Assets what were not afforded the protections in CIP-007-1 R1 and R3. WECC determined that WECC_URE2 was in violation of CIP-006-1 R1.8 because it did not afford its Critical Cyber Assets used in the access control and monitoring of its Physical Security Perimeters the protections in CIP-007-1 R1 and R3. Specifically, WECC_URE2 was in violation of CIP-006-1 R1.8 because it did not test its Critical Cyber Assets to ensure that new Cyber Assets and significant changes to Cyber Assets would not adversely affect existing cyber security controls. Additionally, WECC_URE2 did not evaluate, test, and install applicable security patches for all Cyber Assets as prescribed by CIP-007-1 R3. WECC_URE2 also did not did not implement the protective measures specified in CIP-006-2 R2.	CIP-006-1 (WECC has determined that WECC_URE2 violated CIP-006-1 R1.8 from when the Standard became enforceable for WECC_URE2, until when CIP-006-1 R1.8 was replaced by CIP-006-2 R2.2. Furthermore, WECC_URE2 violated CIP-006-2 R2.2 until when CIP-006-2 R2.2 was replaced by CIP-006-3 R2.2.)	R1; R1.8	Lower	Moderate	WECC determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the bulk power system (BPS). The purpose of this Standard is to identify and protect the Electronic Security Perimeter by protecting all access points on the perimeter. Failure to ensure that Cyber Assets used in the access control and/or monitoring (ACM) of the Electronic Security Perimeter have the appropriate protective measures as specified in CIP-007-1 R1 and R3 may allow unauthorized internal and or external access to these Cyber Assets, which could then allow for successful cyber attacks against Critical Cyber Assets essential for operation of the BPS thereby negatively impacting the operation of the BPS. In this instance, WECC_URE2 failed to ensure that new and changes to Cyber Assets would not have a negative impact on the existing cyber controls and also failed to evaluate, test and install security patches for all Cyber Assets. However, the Cyber Assets were afforded all the remaining protection required by CIP-006-1 R1.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002294	Settlement Agreement	WECC_URE2 self-reported a violation of CIP-007-1 R1. In its Self-Report, WECC_URE2 indicated that, although it has a procedure in place to test security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms before placing software and firmware into production on Critical Cyber Assets, it does not specifically test the software and firmware to determine if significant changes would have adverse effects on cyber security controls. 41 days later, a WECC subject matter expert (SME) held a conference call with WECC_URE2 to confirm the facts contained in WECC_URE2's Self-Report. On the conference call, the WECC SME further clarified that, although WECC_URE2 had existing procedures to test significant changes to ensure there were no existing adverse impacts on functional changes, WECC_URE2 was not testing for significant changes in security controls, as required by the Standard. WECC determined that WECC_URE2 was in violation of CIP-007-1 R1 because it did not have test procedures to ensure that significant changes to existing Cyber Assets within its Electronic Security Perimeter do not adversely affect existing cyber security controls.	CIP-007-1	R1	Medium	High	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2 had substantial testing in place. Although, WECC_URE2 did not test the potential adverse impacts on cyber security controls of significant changes to existing Cyber Assets, WECC_URE2 had existing test procedures in place to test the potential adverse impacts of functional changes.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002295	Settlement Agreement	WECC_URE2 self-reported a violation of CIP-007-1 R3. In its Self-Report, WECC_URE2 explained that it has a patch management program in place to evaluate, test and install applicable security patches for all Cyber Assets which reside its Electronic Security Perimeter. WECC_URE2 further explained that the program was focused only on operating systems and major application patches, but minor, as well as peripheral applications, were not addressed consistently. A WECC subject matter expert (SME) found that although WECC_URE2 had a security patch management program, the program did not track, evaluate, or test applicable ancillary cyber security software. WECC determined that WECC_URE2 is in violation of CIP-007-1 R3 because it failed to establish and document a security patch management program for tracking, evaluating, and testing all of its applicable cyber security software patches for all Cyber Assets within its Electronic Security Perimeter.	CIP-007-1	R3	Lower	Lower	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2 did establish and document a security patch management program. Although the program did not include ancillary cyber security software, and as a result a security weakness could affect all Cyber Assets within the Electronic Security Perimeter if ancillary software is not properly patched, the risk was minimal because WECC_URE2 did have a security patch management program and the Cyber Assets were being afforded the protections in the program.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002396	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). The WECC Audit team (Audit Team) reviewed the documents WECC_URE2 presented as evidence of a Cyber Security Incident response plan and found that the first version of the plan did not include roles and responsibilities or a communication plan as required by CIP-008-1 R1.2. Furthermore, the Cyber Security Incident response plan was updated two more times, and neither of these versions included roles and responsibilities or a communication plan. In addition, the Audit Team noted that version two of CIP-008 requires a Cyber Security Incident response plan to be updated within 30 days of any changes to the plan. WECC_URE2's Cyber Security Incident response plan was not updated to reflect the requirement in version two of CIP-008. WECC determined that WECC_URE2 was in violation of CIP-008-1 R1.2 for not including personnel roles and responsibilities or a communication plan in its Cyber Security Incident response plan. Additionally, WECC determined that WECC_URE2 was in violation of CIP-008-2 R1 for not updating its Cyber Security Incident response plan within 30 days.	CIP-008-1	R1	Lower	High	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2's Cyber Security Incident response plan did identify personnel to be contacted if a Cyber Security Incident did occur.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

PRIVILEGED/CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION (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
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002392	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). To demonstrate its compliance with CIP-003-2 R5, WECC_URE2 provided the WECC Audit team (Audit Team) its Critical Cyber Asset access control program in two documents. The Audit Team found that WECC_URE2's first document did not include the annual verifications required by R5.1.2, R5.2, and R5.3. WECC determined that WECC_URE2 was in violation of CIP-003-2 R5 for not documenting the annual reviews and verifications as required by CIP-003-2 R5.1.2, R5.2 and R5.3.	CIP-003-2	R5	Lower	Moderate	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2 originally documented the annual reviews and verifications required by CIP-003-1 R5.1.2, R5.2 and R5.3 in its access control procedure document. Furthermore, WECC_URE2 did conduct the actually annual reviews and verifications required by CIP-003-2 R5.1.2, R5.2 and R5.3 but simply did not document the reviews and verifications for 2010.	When WECC_URE2 revised its program document and did not include the required annual reviews and verifications	Mitigation Plan completion
Western Electricity Coordinating Council (WECC)	Unidentified Registered Entity 2 (WECC_URE2)	NCRXXXXX	WECC201002395	Settlement Agreement	WECC performed an on-site audit of WECC_URE2's compliance with the Reliability Standards (Audit). The WECC Audit team (Audit Team) requested from WECC_URE2 evidence that it was reviewing, at least annually, its user accounts to verify that access privileges are in accordance with CIP-004-1 R4. At the Audit, WECC_URE2 produced a spreadsheet which demonstrated that WECC_URE2 knew the specific electronic access rights of its personnel; however, this spreadsheet was created at the Audit and did not demonstrate that WECC_URE2 was annually reviewing the electronic access rights of its personnel in accordance with CIP-004-1 R4, as required by CIP-007-1 R5. WECC determined that WECC_URE2 was in violation of CIP-007-1 R5.1.3 for failing to review its user accounts annually to verify they are in accordance with CIP-004-1 R4.	CIP-007-1	R5; R5.1.3	Medium	Severe	WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS) because WECC_URE2 was able to produce a spreadsheet demonstrating that it knew what the electronic access rights of its personnel were even though WECC_URE2 did not review the electronic access rights of its personnel. Although this could have resulted in personnel gaining unauthorized access to WECC_URE2's Electronic Security Perimeters and those unauthorized personnel could possibly present a threat to the reliability of the BPS, this particular violation has a minimal risk because WECC_URE2 knew the electronic access rights of its personnel.	When the Standard became mandatory and enforceable for WECC_URE2	Mitigation Plan completion

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$4,000	Spot Check	MRO_URE1 submitted a Mitigation Plan to address the violation of CIP-007-1 R1. In accordance with the Mitigation Plan, MRO_URE1: (1) ceased the practice of updating anti-virus signatures using a temporary intermediate anti-virus server; (2) revised the EMS anti-virus signature update process and procedure to eliminate the need to introduce a temporary intermediate anti-virus server into the ESP; and (3) reviewed and confirmed all energy management system (EMS) cyber assets are properly identified and protected.	12/31/2010	9/29/2011	Admits	MRO considered MRO_URE1's Internal Compliance Program, which was in place at the time of the violation, to be a mitigating factor when determining the penalty amount.
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	RFC_URE1 separated CIP training from corporate cyber awareness training in order to create a clearer delineation between courses. RFC_URE1 updated its database, which now prevents RFC_URE1 personnel from granting access to CCAs unless a current CIP training date is provided. RFC_URE1 also took direct control over administering CIP training for contractors. Prior to this mitigating action, RFC_URE1 believed its contractors provide RFC_URE1-approved CCA training to their (non-RFC_URE1) employees. Additionally, RFC_URE1 improved its process by developing training lists which will integrate RFC_URE1's Energy Management System cyber access with its physical access lists. The integration of these two lists allows RFC_URE1 to determine which individuals require CIP training and by what deadline. The integration of these two lists allows RFC_URE1 to determine which individuals require CIP training and by what deadline.	5/6/2011	6/9/2011	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and PRA dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	Internal maintenance of PRAs was centralized over one year before the mandatory compliance date of the Standard. At that point, the corporate Human Resources group began collection and storage of all PRAs in an internal electronic database. With this centralization, the risk of misplaced PRAs has been reduced. As discussed in the last column, a system to improve compliance with the Standard is implemented. As all access to CCAs is now centralized, the reporting capabilities that will result from the implementation of this project allows RFC_URE1 to receive alerts of impending expirations of PRAs. Additionally, current PRA dates are automatically available though the integration with other systems. This provides RFC_URE1 with a more comprehensive, proactive approach to the management of PRAs and ensures that future lapses do not occur.	5/6/2011	6/9/2011	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and PRA dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	RFC_URE1 implemented a project to reinforce the timeliness of initiating the personnel change process. In this program, RFC_URE1 implemented a system of checklists to provide consistent steps for transfers and terminations of employees with access to CCAs. This system helps ensure RFC_URE1 removes access to CCAs within the proper time period. Additionally, RFC_URE1 implemented targeted training with management level individuals to help ensure those involved in terminations and transfers are properly trained regarding the relevant requirements and time frames pursuant to CIP-004-1 R4.	5/6/2011	6/9/2011	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and PRA dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	RFC_URE1's corporate entity removed the three CCAs as RFC_URE1 CCAs from its network. Since the devices are no longer CCAs, they are no longer subject to mandatory compliance with CIP-007-2 R4.	11/17/2010	1/11/2012	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and personnel risk assessment dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	RFC_URE1's corporate entity removed the three CCAs as RFC_URE1 CCAs from its network. RFC_URE1 also executed password changes for 90 of the 91 passwords and permanently disabled the remaining account. RFC_URE1 also updated and instituted procedures to improve process controls related to password changes.	11/17/2010	8/3/2011	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and personnel risk assessment dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.
$25,000 (for RFC201000305; RFC201000662; RFC201000306; RFC201100774; RFC201100775; and RFC201100999)	Self-Report	RFC_URE1 implemented an automated log storage process that automatically stores any local event log files for the device on an existing CIP log server and subsequently scans each event for potential incidents. Additionally, RFC_URE1 set logs for a minimum retention period of 90 days. Last, the entity's corporate office completed an extent of condition evaluation to identify possible similar deficiencies for its affiliate CCAs.	12/15/2011	1/31/2012	Agrees/ Stipulates	In assessing the penalty, Reliability*First* favorably considered certain aspects of RFC_URE1's compliance program. Reliability*First* also favorably considered that RFC_URE1 now has a single work flow system to grant or remove access to CCAs, as well as manage employee or contractor transfers and separations in order to improve compliance with the Standard. The system also validates CIP training and personnel risk assessment dates for individuals requesting access to CCAs prior to submitting the access requests to managers for final approval.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$7,500 (for RFC201000646 and RFC2011001073)	Self-Report	RFC_URE2 states that upon discovery, it either removed the individuals' physical access to the CCAs or granted unescorted physical access to the individuals through its CIP access database system. RFC_URE2 completed its total conversion from the paper-based system for granting physical access to the CIP access database system. RFC_URE2 will also use automated systems to collect and document the access rights granted to CCAs.	5/6/2011	11/7/2011	Agrees/ Stipulates	ReliabilityFirst favorably considered certain aspects of RFC_URE2's compliance program. ReliabilityFirst also gave Self-Reporting credit for RFC_URE2.
$7,500 (for RFC201000646 and RFC2011001073)	Self-Report	RFC_URE2 did not submit a separate Mitigation Plan for this violation. ReliabilityFirst determined that the Mitigation Plan for RFC201000646, contained the mitigating activities necessary to resolve the violation of CIP-004-1 R3. RFC_URE2 states that upon discovery, it either removed the individuals' physical access to the CCAs or granted unescorted physical access to the individuals through its CIP access database system. As part of this process, RFC_URE2 removed the physical access rights of the employee at issue.	5/6/2011	11/7/2011	Agrees/ Stipulates	ReliabilityFirst favorably considered certain aspects of RFC_URE2's compliance program. ReliabilityFirst also gave Self-Reporting credit for RFC_URE2.
$15,000 (for RFC201000440, RFC201000441, and RFC201000442)	Self-Report	In the Mitigation Plan, RFC_UREs memorialized the actions they took to address CIP-004-1 R4, including inter alia, an extensive root cause investigation across the RFC_UREs. A full review of all CIP-004 policies and procedures and subsequent changes to add rigor to the program was performed. Revisions to training for all authorizers and performers responsible for assuring CIP-004 compliance were added, including the addition of an annual requirement. A task force for routine assessments of some of the key tools used to implement the program was also created.	2/29/2012 (Approved Date)	TBD	Neither Admits nor Denies	Reliability*First* considered certain aspects of the RFC_UREs' compliance program as mitigating factors. In addition, Reliability*First* also considered the quick response by the RFC_UREs to the identification of the incidents, the implementation of immediate remediation actions including interim processes consisting of significant manual controls and levels of cross-checks, the dedication of a cross-functional team to a full investigation of the entire CIP-004 program and the subsequent development and implementation of a comprehensive mitigation plan.
$15,000 (for RFC201000440, RFC201000441, and RFC201000442)	Self-Report	In the Mitigation Plan, RFC_UREs memorialized the actions they took to address CIP-004-1 R4, including inter alia, an extensive root cause investigation across the RFC_UREs. A full review of all CIP-004 policies and procedures and subsequent changes to add rigor to the program was performed. Revisions to training for all authorizers and performers responsible for assuring CIP-004 compliance were added, including the addition of an annual requirement. A task force for routine assessments of some of the key tools used to implement the program was also created.	2/29/2012 (Approved Date)	TBD	Neither Admits nor Denies	Reliability*First* considered certain aspects of the RFC_UREs' compliance program as mitigating factors. In addition, Reliability*First* also considered the quick response by the RFC_UREs to the identification of the incidents, the implementation of immediate remediation actions including interim processes consisting of significant manual controls and levels of cross-checks, the dedication of a cross-functional team to a full investigation of the entire CIP-004 program and the subsequent development and implementation of a comprehensive mitigation plan.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$15,000 (for RFC201000440, RFC201000441, and RFC201000442)	Self-Report	In the Mitigation Plan, RFC_UREs memorialized the actions they took to address CIP-004-1 R4, including inter alia, an extensive root cause investigation across the RFC_UREs. A full review of all CIP-004 policies and procedures and subsequent changes to add rigor to the program was performed. Revisions to training for all authorizers and performers responsible for assuring CIP-004 compliance were added, including the addition of an annual requirement. A task force for routine assessments of some of the key tools used to implement the program was also created.	2/29/2012 (Approved Date)	TBD	Neither Admits nor Denies	ReliabilityFirst considered certain aspects of the RFC_UREs' compliance program as mitigating factors. In addition, ReliabilityFirst also considered the quick response by the RFC_UREs to the identification of the incidents, the implementation of immediate remediation actions including interim processes consisting of significant manual controls and levels of cross-checks, the dedication of a cross-functional team to a full investigation of the entire CIP-004 program and the subsequent development and implementation of a comprehensive mitigation plan.
$9,000	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to address the violation of CIP-003-1 R1. In accordance with the Mitigation Plan, Texas RE_URE1 conducted two main activities. First, Texas RE_URE1 mailed a copy of the cyber security policy to each contractor with remote authorized cyber access. Second, Texas RE_URE1 placed a copy of the cyber security policy at a central location of each Critical Asset within the Texas RE region and explained on the Physical Security Perimeters' sign-in, sign out logs the availability of the cyber security policy.	9/1/2010	5/31/2011	Admits	Texas RE considered that Texas RE_URE1 had an internal compliance program, in place at the time of the violation, as a mitigating factor when determining the penalty amount.
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Report	WECC_URE1 submitted a Mitigation Plan, stating an automated Supervisory Control and Data Acquisition Systems (SCADA) calculation was implemented, which triggers the receipt of the WECC RC Time Error every day, calculates the difference between the required time values, and documents it in WECC_URE1's system.	12/15/2010	11/16/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Report	WECC_URE1 submitted a Mitigation Plan, stating that it completed the following actions: 1) trained all individuals who lacked initial or annual training; 2) revoked access for individuals who no longer required access; 3) updated its procedures for training newly-hired employees; 4) updated its procedures to conduct annual training for all employees once a year regardless of the original training date; 5) consolidated two training sessions into a single training each year; and 6) trained process members of new procedures.	5/13/2011	9/1/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Certification	WECC_URE1 submitted a Mitigation Plan, outlining the following mitigating actions: 1) for CIP-005 R3- deployed a system to provide monitoring and logging of access-to-access points at all times. The system is configured to alert designated personnel of attempted or actual unauthorized access. In addition, some documentation recording measures were put in place; 2) for CIP-007 R3- documented an assessment for applicability of security patches within 30 days of the patch being made available; 3) for CIP-009 R4- included backup and restored procedures for its seven Physical Access Control and Monitoring (ACM) control Panels in its Recovery Plan; 4) for CIP-009- R5- included annual testing of information essential to recovery that it stored on backup media.	3/25/2011	7/21/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Certification	WECC_URE1 submitted a Mitigation Plan, stating that it had completed the following actions: 1) set up an automatic notification of security patch releases from its vendors; 2) purchased a software tool, which ensures that the process owner has the ability to track and audit the completion of these tasks within 30 calendar days.	4/15/2011	12/7/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Report	WECC_URE1 submitted a Mitigation Plan, committing to the following actions: 1) WECC_URE1 followed its Cyber Security Event Procedure when replacing or receiving new Cyber Assets; 2) implement a manual alert-to-auto alert timelines for CIP requirements; 3) conduct a weekly log review with process owners, retains logs for 90 days; and 4) create new documents outlining the process and method used for monitoring the logging for new assets.	3/18/2011	12/7/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Certification	WECC_URE1 submitted a Mitigation Plan, stating that WECC_URE1 performed an assessment on the system and developed a task management software system to help track deadlines and train users on the new tracking software system.	4/1/2011	6/30/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$45,000 (for WECC201002604, WECC201102807, WECC201102599, WECC201102609, WECC201102606, WECC201102613, and WECC200901475)	Self-Report	WECC_URE1 submitted a Mitigation Plan and two subsequent revised plans . According to its plan, WECC_URE1: 1) changed its vendor, with the new vendor providing full service to WECC_URE1; 2) completed testing and validated its new system with the new vendor, which ensured that WECC_URE1 could respond to requests from an Interchange Authority to transition an Arranged Interchange to a Confirmed Interchange before the e-tag expired.	8/2/2010	8/12/2011	Agrees/ Stipulates	WECC reviewed WECC_URE1's Internal Compliance Program and considered it a mitigating factor in determining the penalty amount.
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	1. WECC_URE2 continues to operate under its AGC procedure, which directs operators to notify the Adjacent BAs and Reliability Coordinator if the ATEC is disabled for any reason. 2. WECC_URE2 issued a critical communication message. A critical communication is a message sent out in order to communicate and inform operating personnel of information which is critical to operating the system. Critical communication messages also document the receipt and understanding by noting which personnel have read, have not read, and if any have questions concerning the communication. 3. In response to the violation, WECC_URE2 has created an alarm for the AGC as follows: When the AGC system is functioning in any mode except ATEC mode, the following alarm is to be generated: "AGC in NON-ATEC Mode, Send WECC Message Immediately." WECC RC's messaging system, in turn, automatically retransmits the message to its subscribers which include the region's BAs.	4/21/2011	1/25/2012	Agrees/ Stipulates	
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2 attended a WECC-organized Critical Infrastructure Protection User Group meeting. At that meeting, WECC staff explained the WECC view that "The cyber security policy must address all requirements in the Standard CIP-002 through CIP-009" and not merely a statement that the entity will comply with all requirements in CIP-002 through CIP-009. Upon receipt of this WECC guidance, WECC_URE2 promptly modified its policy accordingly. WECC_URE2 updated its policy to address each requirement individually. The policy is directive in nature and tailored to how management intends WECC_URE2 to go about addressing each requirement individually.	8/30/2010	7/7/2011	Neither Admits nor Denies	
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2 modified its document to include a configuration management process. Additionally WECC_URE2 purchased a product which assists in properly documenting and implementing configuration management activities in order to enhance WECC_URE2's efforts to adhere to the requirements set forth by CIP-003-1 R6. This product is now part of the documented configuration management process.	5/24/2010	7/7/2011	Agrees/ Stipulates	

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Self-Report	WECC_URE2 completed the following mitigation actions: 1. Personnel access lists to CCAs have been reviewed to re-evaluate the business need for access. 2. Improved software queries have been developed to eliminate duplicative training records and clearly identify personnel that are within 30 days of their cyber security training expiration date. These personnel are notified and flagged as requiring training. They are rechecked within 7 days of their training expiration date. If they have not completed their training, their access is revoked until their training is completed; 3. Verification of cyber security training dates is independently reviewed by two WECC_URE2 employees; 4. September 1st of each year was established as the annual retraining date for all personnel that have access to WECC_URE2's CCAs; 5. Additional fields were added to the cyber security training database that will decrease duplication of records for individuals who have taken cyber security training and allow removal of individuals from the list by indicating that training is no longer needed due to transfer or termination; 6. Created and maintained a unique identifier for personnel, contactors and any other personnel in the training database, reducing the risk of human error by reducing the manual processes required in cross-referencing data; and 7. Created an automatic annual training notification. This provided an automatic mechanism to notify personnel that renewal of training is required and CCA access needs to be revoked for personnel whose training has not been renewed within a predetermined time prior to the training expiration date.	4/20/2010	11/30/2010	Agrees/ Stipulates	When assessing the penalty, WECC did not apply any self-reporting credit since WECC_URE2 self-reported during its self-certification period.
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2's Mitigation Plan required it to improve its access rights review process. The new process links specifically-defined electronic access rights to specific user roles. Each role is directly associated with a specific job function. WECC_URE2 management will approve the access rights associated with an individual role and assign the roles to personnel as required. WECC_URE2 will review and validate the specific access rights associated with each individual user on a quarterly basis.	9/1/2011	9/15/2011	Agrees/ Stipulates	WECC assessed a single aggregate penalty for WECC_URE2's violations of CIP-004-1 R4 and CIP-007-1 R5.1.3. WECC_URE2's failure to perform annual reviews of its electronic access rights is a single incidence of noncompliance that resulted in a violation of CIP-007-1 R5.1.3. WECC determined WECC_URE2's failure to perform annual reviews of electronic access rights resulted in WECC_URE2's violations of CIP-004-1 R4 and CIP-007-1 R5.3.1. Accordingly, the penalty assessed for CIP-004-1 R4 is a single penalty representative of the aggregate of the related violations.
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Self-Report	WECC_URE2's Mitigation Plan required it to reevaluate its test procedures to test that new and significant changes to cyber assets do not adversely affect existing security controls to meet the requirements of CIP-007 R1, as well as refine its patch management process to meet the requirements of CIP-007 R3.	10/15/2010	5/17/2011	Agrees/ Stipulates	When assessing the penalty, WECC did not apply any self-reporting credit since WECC_URE2 reported during its self-certification period.

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Self-Report	The CIP-006-1 R1.8 Mitigation Plan addressed the issues with CIP-007-1. WECC_URE2 developed and enhanced existing processes to address security control testing and patch management. This along with establishing a test environment for performing these processes and enhancing the production environment fully met the requirement. The following actions were taken: 1. Implemented new test environment for security patch management and security control testing prior to any significant changes or upgrades to the physical access control system; 2. Enhanced production environment by making changes in order to utilize and streamline the security patch process and security controls testing; 3. Implemented and utilized enhanced security patch process; and 4. Established processes for security control testing which will be used to baseline the physical access control system configuration enabling security control testing in the new environment prior to updating production.	12/6/2010	5/26/2011	Agrees/ Stipulates	When assessing the penalty, WECC did not apply any self-reporting credit since WECC_URE2 self-reported during its self-certification period. WECC assessed a single aggregate penalty for WECC_URE2's violations of CIP-006-1 R1.8 and CIP-007-1 R1 and R3. WECC_URE2's failure to provide the protections in CIP-007-1 R1 and R3 to the ACM Cyber Assets is a single incidence of noncompliance that resulted in violations of CIP-007-1 R1 and R3. Accordingly, the penalty assessed for CIP-006-1 R1.8 is a single penalty representative of the aggregate of the related violations.
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Self-Report	Pursuant to WECC_URE2's Mitigation Plan, WECC_URE2 has developed new test procedures to test the adverse impacts on security controls of significant changes to Cyber Assets.	7/29/2010	5/17/2011	Agrees/ Stipulates	WECC assessed a single aggregate penalty for WECC_URE2's violations of CIP-005-1 R1.5, CIP-006-1 R1.8 and CIP-007-1 R1. WECC_URE2's failure to provide the protections in CIP-007-1 to its Critical Cyber Assets is a single incidence of noncompliance that resulted in violations of CIP-005-1 R1.5 and CIP-006-1 R1.8. Accordingly, the penalty assessed for CIP-007-1 R1 is a single penalty representative of the aggregate of the related violations
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Self-Report	In order to mitigate its violation, WECC_URE2 implemented an automated solution for identifying changes which affect WECC_URE2's security posture. WECC_URE2 refined its security patch management process to fully meet the requirements of the Standard by implementing the following actions: 1. Inventory all operating systems and applications that reside on Cyber Assets within the Electronic Security Perimeters; and 2. Enhance the program to track, evaluate, test and install security patches for all identified operating systems and applications that reside on Cyber Assets within the Electronic Security Perimeters.	10/15/2010	10/31/2011	Agrees/ Stipulates	WECC assessed a single aggregate penalty for WECC_URE2's violations of CIP-005-1 R1.5, CIP-006-1 R1.8 and CIP-007-1 R3. WECC_URE2's failure to provide the protections in CIP-007-1 to its Cyber Assets is a single incidence of noncompliance that resulted in violations of CIP-005-1 R1.5 and CIP-006-1 R1.8. Accordingly, the penalty assessed for CIP-007-1 R3 is a single penalty representative of the aggregate of the related violations
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2's Mitigation Plan required it to modify its Cyber Security Incident response plan to include a section devoted to roles and responsibilities that details the identification of specific employee positions that are the primary "owners" or designated lead personnel for the maintenance, protection and use of NERC CIP assets. Additionally, WECC_URE2's Mitigation Plan required it to add a section to address a communications plan and a procedure for updating the document within 30 days.	6/30/2010	7/8/2011	Neither Admits nor Denies	

Attachment A-2

January 31, 2012 Public Spreadsheet Notice of Penalty Spreadsheet

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

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"	Factors Affecting the Penalty and Other Considerations
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2's Mitigation Plan required it to update its cyber security plan for managing access to protected Critical Cyber Asset information, to require annual reviews and verifications as required by CIP-003-2 R5.1.2, R5.2 and R5.3. WECC_URE2 also communicated the document changes to the appropriate areas and had the appointed compliance manager approve and sign the revised document.	7/30/2011	8/19/2011	Agrees/ Stipulates	
$55,000 (for WECC201002246; WECC201002391; WECC201002393; WECC201002296; WECC201002394; WECC201002399; WECC201002397; WECC201002294; WECC201002295; WECC201002396; WECC201002392; and WECC201002395)	Audit	WECC_URE2's Mitigation Plan required it to update its quarterly review process to review specific access rights in accordance with CIP-007-1 R5.	9/1/2011	9/15/2011	Agrees/ Stipulates	WECC assessed a single aggregate penalty for WECC_URE2's violations of CIP-004-1 R4 and CIP-007-1 R5.1.3. WECC_URE2's failure to perform annual reviews of its electronic access rights is a single incidence of noncompliance that resulted in a violation of CIP-007-1 R5.1.3. WECC determined WECC_URE2's failure to perform annual reviews of electronic access rights resulted in WECC_URE2's violations of CIP-004-1 R4 and CIP-007-1 R5.3.1. Accordingly, the penalty assessed for CIP-004-1 R4 is a single penalty representative of the aggregate of the related violations.

Document Accession #: 20120215-5145 **Filed Date: 02/15/2012**

Document Content(s)