Federal Energy Regulatory Commission
Washington, D.C. 20426
May 28, 2021

Re:
Twenty Fourth Response Letter
FOIA No. FY19-30

VIA ELECTRONIC MAIL ONLY
Michael Mabee

CivilDevenseBook@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 letters dated May 19, 2021 and May 21, 2021, the submitter and certain concerned Unidentified Registered Entities (URE) were informed that a copy of the public version of the Notices of Penalty associated with Docket Nos. NP12-10 and NP11-253, along with the names of certain relevant UREs inserted on the first page, would be disclosed to you no sooner than five calendar days from that date. *See* 18 C.F.R. § 388.112(e).[2] The five-day notice period has elapsed and the documents are enclosed.

On November 18, 2019, you filed suit in the U.S. District Court for the District of Columbia asserting claims in connection with this FOIA request. *See Mabee v. Fed. Energy Reg. Comm'n.,* Civil Action No. 19-3448 (KBJ) (D.D.C.). Because this FOIA request is currently in litigation, this letter does not contain information regarding administrative appeal of the response to the FOIA request. For any further assistance or 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] NP12-10 and NP11-253 are spreadsheet NOP dockets and notification of the FOIA request as well as the Notice of Intent to Release were only sent to those UREs for whom FERC determined that disclosure of their identities was appropriate.

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

Sincerely,

SARAH VENUTO

Digitally signed by SARAH VENUTO
Date: 2021.05.28 20:56:17 -04'00'

Sarah Venuto
Director
Office of External Affairs

Enclosure

cc:

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

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

Bcc: Relevant UREs

NP11-253

see .pdf page range 24-28:

-NextEra Energy Resources, LLC (NextEra)

-Town of Winterville (Winterville)

-Town of Sharpsburg (Sharpsburg)

-Town of Stantonsburg (Stantonsburg)

July 29, 2011

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides the attached Administrative Citation Notice of Penalty for July 2011[1] (July 2011 Administrative Citation NOP) in Attachment A regarding 20 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 July 2011 Administrative Citation NOP resolves 38 violations[5] of 15 Reliability Standards. The violations in this NOP did not have a serious or substantial impact on the reliability of the bulk power system (BPS). In all cases, the violations contained in this NOP have been fully mitigated.

Some of the violations at issue in the July 2011 Administrative Citation NOP are being filed with the Commission because the Regional Entities have respectively entered into agreements with the Registered Entities identified in Attachment A to resolve all outstanding issues arising from preliminary and non-public assessments resulting in the Regional Entities' determination and

---

[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.

116-390 Village Blvd.
Princeton, NJ 08540
609.452.8060 | www.nerc.com

findings of the enforceable violation of the Reliability Standards identified in Attachment A. In some of those settlement agreements, 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 or do not contest the violations. While some of the Registered Entities have neither admitted nor denied or do not contest the violations of the Reliability Standards, they have agreed to the proposed penalty stated in Attachment A, in addition to other remedies and mitigation actions to mitigate the instant violation and ensure future compliance with the Reliability Standards. Accordingly, all of the violations, identified as NERC Violation Tracking Identification Numbers in Attachment A, are being filed in accordance with the NERC Rules of Procedure and the CMEP.

As discussed below, this July 2011 Administrative Citation NOP resolves 38 violations. The Commission has encouraged the use of a streamlined enforcement process that could avoid the filing of individual notices of penalty for violations that did not pose a serious or substantial risk to the BPS.[6] Completing these non-serious violations will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards. NERC respectfully requests that the Commission accept this July 2011 Administrative Citation NOP.

Statement of Findings Underlying the Alleged Violations

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

This filing contains the basis for approval by the NERC of the findings and penalties reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2010), 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 July 2011 Administrative Citation 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.

Status of Mitigation[7]

As noted above and reflected in Attachment A, the respective Regional Entities have determined that the violations identified in Attachment A have been mitigated. The mitigation activities have all been accepted by the Regional Entity and verified as completed. These activities are described in Attachment A for each respective violation. Information also is provided regarding the dates of Regional Entity verification of such completion.

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

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed[8]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,[9] NERC reviewed the July 2011 Administrative Citation NOP and the attachments thereto. NERC approved the Administrative Citation Spreadsheet, including the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, NERC'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 penalty 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.

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.

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

Attachments to be included as Part of this Notice of Penalty

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

a) Administrative Citation Spreadsheet, included as Attachment A;

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

c) VRF Revision History Applicable to the Administrative Citation NOP, included as Attachment C.

A Form of Notice Suitable for Publication[10]

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

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 Administrative Citation NOP:

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 116-390 Village Boulevard Princeton, New Jersey 08540-5721 (609) 452-8060 (609) 452-9550 – facsimile david.cook@nerc.net *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list. *See also* Attachment B for additions to the service list.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, D.C. 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net

[10] *See* 18 C.F.R § 39.7(d)(6).

Conclusion

Handling these violations in a streamlined process will help NERC and the Regional Entities focus on the more serious violations of the mandatory and enforceable NERC Reliability Standards. Accordingly, NERC respectfully requests that the Commission accept this Administrative Citation 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
David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
116-390 Village Boulevard
Princeton, NJ 08540-5721
(609) 452-8060
(609) 452-9550 – facsimile
david.cook@nerc.net

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

cc: Entities listed in Attachment B

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment A

Administrative Citation Spreadsheet (Included in a Separate Document)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment B

Additions to the service list

ATTACHMENT B

REGIONAL ENTITY SERVICE LIST FOR JULY 2011 ADMINISTRATIVE CITATION NOTICE OF PENALTY

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

Richard Gilbert*
Manager of Compliance Enforcement
Florida Reliability Coordinating Council, Inc.
3000 Bayport Drive, Suite 690
Tampa, Florida 33607-8402
(813) 207-7991
(813) 289-5648 – facsimile
rgilbert@frcc.com

FOR MRO:

Daniel P. Skaar*
President
Midwest Reliability Organization
2774 Cleveland Avenue North
Roseville, MN 55113
P: (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
P: (651) 855-1708
se.patrick@midwestreliability.org

FOR NPCC:

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

FOR SERC:

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

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

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

FOR 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
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment C

VRF Revision History Applicable to the Administrative Citation NOP

ATTACHMENT C

Violation Risk Factor Revision History Applicable to the Administrative Citation Notice of Penalty

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

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

- CIP-003-1 R1 has a Medium VRF; R1.1, R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

- CIP-003-1 R2 has a Medium VRF; R2.1, R2.2 and R2.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R2 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-003-1 R2 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

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

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

- CIP-004-1 R4 and R4.1 each have a Lower VRF; R4.2 has a "Medium" VRF. When NERC filed VRFs, it originally assigned CIP-004-1 R4.2 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on January 27, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-004-1 R4.2 was in effect from June 18, 2007 until January 27, 2009 when the Medium VRF became effective.

- When NERC filed VRFs it originally assigned CIP-006-1 R1.5 a Lower VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for CIP-006-1 R1.5 was in effect from June 18, 2007 until February 2, 2009 when the Medium VRF became effective. CIP-006-1 R1, 1.1, 1.2, 1.3, 1.4, 1.6 have Medium VRFs and CIP-006-1 R1.7, 1.8 and 1.9 have Lower VRFs.

- 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 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 R4 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-007-1 R4 was in effect from June 18, 2007 until February 2, 2009, when the Medium VRF became effective. The VRFs for CIP-007-2 R4 and CIP-007-3 R4 were not changed when CIP-007-2 went into effect on April 1, 2010 and when CIP-007-3 went into effect on October 1, 2010.

- When NERC filed VRFs for FAC-008-1, NERC originally assigned Lower VRFs to FAC-008-1 R1.1, R1.2, R1.2.1 and R1.2.2. The Commission approved the VRFs but directed modifications. On December 19, 2007, NERC filed the modified Medium VRFs for FAC-008-1 R1.1, R1.2, R1.2.1 and R1.2.2 for

approval. On February 6, 2008, the Commission issued an Order approving the modified 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 and the Medium VRFs has been in effect since February 6, 2008. FAC-008-1 R1, R1.3 and R1.3.5 have Lower VRFs and R1.3.1, R1.3.2, R1.3.3 and R1.3.4 have Medium VRFs.

- Reliability Standard PER-002-0 R3 has a High VRF, sub-requirements R3.1 and R3.2 have Medium VRFs and sub-requirements R3.3 and R3.4 have Lower VRFs.

- When NERC filed VRFs 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-005-1 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.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Attachment D

Notice of Filing

ATTACHMENT D

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

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

NOTICE OF FILING
July 29, 2011

Take notice that on July 29, 2011, the North American Electric Reliability Corporation (NERC) filed an Administrative Citation Notice of Penalty regarding twenty (20) 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

July 29, 2011 Public Spreadsheet - Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	Florida Public Utilities Company (FPUC)	NCR00025	FRCC200800143	Settlement Agreement	FPUC, as a Transmission Owner, had not established its methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities per R1.	FAC-008-1	1	Medium	Severe	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because FPUC was operating its equipment using manufacturer's equipment ratings. In 2001-2003, there was an engineering redesign to the line and substation to add a second parallel line. Since 2003, there have been no significant changes to the design of the equipment. Finally, the entity is very small with 39 square miles of service territory, less than 100 MW of load and only 8.1 miles of parallel transmission line with only one substation.	6/18/2007	12/12/2008	$4,500 (Settlement of FRCC200800143, FRCC200800153 and FRCC201000372)	Self-Certification	Established its current methodology used for developing Facility Ratings (Facility Ratings Methodology) of its solely and jointly owned Facilities per R1.	12/12/2008	2/28/2009	Neither Admits nor Denies
FRCC	Florida Public Utilities Company (FPUC)	NCR00025	FRCC200800153	Settlement Agreement	FPUC, as a Transmission Owner, did not have a Protection System maintenance and testing program for Protection Systems that affect the reliability of the bulk power system (BPS) that included (R1.1) maintenance and testing intervals and their basis and (R1.2) summary of maintenance and testing procedures.	PRC-005-1	1 (1.1, 1.2)	High	Severe	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because routine testing and maintenance according to the manufacturers recommendations had been performed and FPUC did have documentation that testing was performed. In addition the Protection System components were all newly installed in 2003-2004. The entity also performed weekly inspections of the substation Protective System equipment. Finally, the entity is very small with 39 square miles of service territory, less than 100 MW of load and only 8.1 miles of parallel transmission line with only one substation.	6/18/2007	12/2/2008	$4,500 (Settlement of FRCC200800143, FRCC200800153 and FRCC201000372)	Self-Certification	Developed a Protection System maintenance and testing program for Protection Systems that affects the reliability of the bulk power system (BPS) including (R1.1) maintenance and testing intervals and their basis and (R1.2) summary of maintenance and testing procedures.	12/2/2008	12/18/2009	Neither Admits nor Denies
FRCC	Florida Public Utilities Company (FPUC)	NCR00025	FRCC201000372	Settlement Agreement	FPUC, as a Transmission Owner (TO), did not create, maintain or publish a facility connection requirements document to ensure compliance with NERC Reliability Standards.	FAC-001-0	1	Medium	Severe	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because all applicable subrequirements would have been discussed and negotiated during the engineering studies related to the interconnection. In addition no interconnections were made during the time period of the violation 6/18/07 to 5/31/08. Also, 95% of the applicable transmission line is not contained within the entity's territory. Further, an existing Network Operating Agreement with the adjacent TO would have required notification and an engineering study prior to any interconnection. Finally the entity is very small with 39 square miles of service territory, less than 100 MW of load and only 8.1 miles of parallel transmission line with only one substation.	6/18/2007	5/31/2008	$4,500 (Settlement of FRCC200800143, FRCC200800153 and FRCC201000372)	Audit	Developed a facility connection requirements document per R1.	5/31/2008	7/14/2010	Neither Admits nor Denies
FRCC	Florida Keys Electric Cooperative Assn (FKEC)	NCR00021	FRCC200900290	Settlement Agreement	FKEC, as a Transmission Owner, had documented and maintained facility connection requirements but failed to publish the document (publicly post).	FAC-001-0	1	Medium	Moderate	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the entity had provided its facility connection requirements document to the RC, BAs and TOPs through a secured Web site even though it had not posted the document publicly. In addition there were no requests for facility interconnections during this time period.	6/18/2007	12/14/2009	$1,500 (Settlement of FRCC200900290, FRCC200900291, FRCC200900292)	Audit (12/11/2009)	Updated FKEC's Web site adding *FKEC Facility Connection Requirements* .	12/14/2009	1/19/2010	Neither Admits nor Denies
FRCC	Florida Keys Electric Cooperative Assn (FKEC)	NCR00021	FRCC200900291	Settlement Agreement	FKEC's transmission Facility Ratings Methodology did not include all of the subrequirements (did not address the scope of the Rating that addresses and includes at a minimum Normal and Emergency Ratings, Ratings provided by equipment manufacturers, design criteria, ambient conditions, operating conditions and any other assumptions) for relay protective devices (R1.2.1, 1.2.2, 1.3).	FAC-008-1	1 (1.2.1, 1.2.2, 1.3)	Medium	Moderate	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because FKEC's documented Facility Ratings Methodology included a statement that it was their design principle that relay protective device settings not be limiting factors on their transmission system. In addition, the entity was operating its equipment within manufacturer's recommendations.	6/18/2007	12/11/2009	$1,500 (Settlement of FRCC200900290, FRCC200900291, FRCC200900292)	Audit (12/11/2009)	1. Update FKEC policy *FAC-008-1 Facility Ratings Methodology* to include required relay protective devices. 2. Updated the FRCC ROG Web site with the updated FKEC Facility Ratings Methodology document.	12/11/2009	1/19/2010	Neither Admits nor Denies
FRCC	Florida Keys Electric Cooperative Assn (FKEC)	NCR00021	FRCC200900292	Settlement Agreement	FKEC's evidence was insufficient to demonstrate that its training staff had knowledge of instructional capabilities from June 18, 2007 to March 24, 2009.	PER-002-0	3.4	Lower	Moderate	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the training staff was competent in the knowledge of system operations and FKEC had trained employees in the past but lacked documentation of instructional capability.	6/18/2007	3/24/2009	$1,500 (Settlement of FRCC200900290, FRCC200900291, FRCC200900292)	Audit (12/11/2009)	FKEC's Supervisor of System Operations received NERC-approved "Train-the-Trainer" certification on 3/24/2009.	3/24/2009	1/19/2010	Neither Admits nor Denies
NPCC	Boralex Stratton Energy, LP (Boralex)	NCR10352	NPCC201000209	NOCV	During the March 2010 off-site compliance audit, Boralex failed to provide documented (either electronic or hard copy) procedure for the recognition of and for making its operating personnel aware of sabotage events at its two generating facilities as required by R1.	CIP-001-1	1	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) based on the size of the two Boralex generating sites that lacked the sabotage procedure (respectively 55 MW and 44 MW). There was no actual impact to the bulk electric system as there was not an event on the ISO-NE system where the lack of the proper Boralex sabotage procedure played a role.	8/14/2009	3/31/2011	$5000 (Settlement of NPCC201000209, NPCC201000210, NPCC201000211, and NPCC201000212)	Audit	1. Boralex created a proper sabotage reporting procedure to meet CIP-001-1 R1 through R4 for both generating sites. 2. Boralex provided training on the sabotage procedure to operating personnel at both generating sites.	3/31/2011	4/7/2011	Admits

Attachment A-1

July 29, 2011 Public Spreadsheet - Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
NPCC	Boralex Stratton Energy, LP (Boralex)	NCR10352	NPCC201000210	NOCV	During the March 2010 off-site compliance audit, Boralex failed to provide documented procedure for communicating information concerning sabotage events to appropriate parties in the Interconnection as required by R2.	CIP-001-1	2	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) based on the size of the two Boralex generating sites that lacked the sabotage procedure (respectively 55 MW and 44 MW). There was no actual impact to the bulk electric system as there was not an event on the ISO-NE system where the lack of the proper Boralex sabotage procedure played a role.	8/14/2009	3/31/2011	$5000 (Settlement of NPCC201000209, NPCC201000210, NPCC201000211, and NPCC201000212)	Audit	1. Boralex created a proper sabotage reporting procedure to meet CIP-001-1 R1 through R4 for both generating sites. 2. Boralex provided training on the sabotage procedure to operating personnel at both generating sites.	3/31/2011	4/7/2011	Admits
NPCC	Boralex Stratton Energy, LP (Boralex)	NCR10352	NPCC201000211	NOCV	During the March 2010 off-site compliance audit, Boralex failed to provide documented sabotage response guidelines, including personnel to contact for reporting disturbances due to sabotage events as required by R3.	CIP-001-1	3	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) based on the size of the two Boralex generating sites that lacked the sabotage procedure (respectively 55 MW and 44 MW). There was no actual impact to the bulk electric system as there was not an event on the ISO-NE system where the lack of the proper Boralex sabotage procedure played a role.	8/14/2009	3/31/2011	$5000 (Settlement of NPCC201000209, NPCC201000210, NPCC201000211, and NPCC201000212)	Audit	1. Boralex created a proper sabotage reporting procedure to meet CIP-001-1 R1 through R4 for both generating sites. 2. Boralex provided training on the sabotage procedure to operating personnel at both generating sites.	3/31/2011	4/7/2011	Admits
NPCC	Boralex Stratton Energy, LP (Boralex)	NCR10352	NPCC201000212	NOCV	During the March 2010 off-site compliance audit, Boralex failed to provide documented evidence that it had established communications contacts with local FBI officials and documented reporting procedures as required by R4.	CIP-001-1	4	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) based on the size of the two Boralex generating sites that lacked the sabotage procedure (respectively 55 MW and 44 MW). There was no actual impact to the bulk electric system as there was not an event on the ISO-NE system where the lack of the proper Boralex sabotage procedure played a role.	8/14/2009	3/31/2011	$5000 (Settlement of NPCC201000209, NPCC201000210, NPCC201000211, and NPCC201000212)	Audit	1. Boralex created a proper sabotage reporting procedure to meet CIP-001-1 R1 through R4 for both generating sites. 2. Boralex provided training on the sabotage procedure to operating personnel at both generating sites.	3/31/2011	4/7/2011	Admits
NPCC	Millennium Power Partners, LP (MPP)	NCR07144	NPCC201000216	NOCV	MPP self-reported that on 12/1/10 at 2353 hours, the control room operator at MPP received two alarms that the combustion turbine (CT) automatic voltage regulator (AVR) had automatically reverted to manual mode from automatic mode. Operating personnel attempted to immediately reset the CT AVR to restore it to the automatic mode. After several attempts, they were still unsuccessful. After a phone call to a supervisor was made for guidance, the CT AVR was restored to automatic mode at 0046 hours on 12/2/10. The steam turbine (ST) AVR remained in automatic mode for the duration of the incident. NPCC Enforcement found MPP in violation of VAR-002-1.1b R3.1 for failing to notify ISO-NE within 30 minutes of the change of status of the AVR. ISO-NE, the Transmission Operator, was notified of the AVR status change and restoration on 12/2/10.	VAR-002-1.1b	3.1	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The violation created a minimal potential risk to the ISO-NE system while the CT AVR was in a state where it was unable to respond in an automatic fashion. The violation created minimal actual risk as the MPP control room operator maintained proper voltage manually during the 53 minutes that the CT AVR was not in automatic mode.	12/2/2010	12/2/2010	$0	Self-Report	1. In the immediate timeframe after the violation, all MPP operating personnel were verbally instructed to notify ISO-NE via the automatic ring down phone located in the control room every time there is a status change the automatic voltage regulator (AVR) for the combustion turbine (CT) or the steam turbine (ST). Operating personnel were also instructed to contact ISO-NE whether or not the issue was resolved within 30 minutes. 2. Training material relating to the VAR standard requirements and other NERC standards was presented to all plant personnel. The material placed special emphasis on VAR-002 and the reason for the Self-Report. 3. Installed new alarms that direct plant operators to contact ISO-NE and the Rhode Island-Eastern Massachusetts-Vermont Energy Control. REMVEC operates as a satellite of the New England Power Exchange (NEPEX) which coordinates and directs the operation of all major electric power and generation facilities in the New England area.	12/16/2010	2/17/2011	Admits
NPCC	United Illuminating Company	NCR07222	NPCC201100233	Settlement Agreement	Two electronic relays for a 115 kV transmission line were not maintained within the defined interval. The relays were placed in service in May 2001 and should have been maintained in 2007 per the six-year maintenance interval. The relays should have been maintained no later than December 31, 2007. The relays were not maintained until August 31, 2010. The primary cause was determined to be the lack of establishment of a maintenance work plan at the time of installation.	PRC-005-1	2	High	Lower	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system. There are electromechanical relays installed as backup protection. There were no misoperations of the protection system between June 2007 and August 2010. There is no record of a fault on the line during this period. Both relays were found to have been set properly and functioning properly when the entity ultimately performed maintenance and testing.	1/1/2008	8/31/2010	$2,500	Self-Report	1. Performed maintenance on protection devices that were missed. 2. Added a step to the maintenance plan to enhance the communication between Engineering adding devices and System Maintenance establishing work plans.	1/7/2011	6/3/2011	Does Not Contest
MRO	Rochester Public Utilities (RPU)	NCR01027	MRO201100308	NOCV	On April 7, 2011, RPU self-reported noncompliance with Reliability Standard FAC-009-1 R1 because its substation bus jumpers did not meet the thermal ratings for certain scenarios as established in ANSI and IEEE standards cited within RPU's Facility Ratings Methodology. RPU failed to use the appropriate thermal rating for jumper conductors within a substation that connects circuit breaker bushings to disconnect switch terminal pads. These jumpers have been in service since 2002.	FAC-009-1	1	Medium	Lower	MRO determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the existing jumpers are limited to below 1,200 amps only at high ambient summer temperatures. The full 1,200 amp duty is only required when the RPU ring bus is open. Additionally, the peak load for RPU is approximately 280 MW. RPU has two 161 kV interconnection points and the RPU transmission system is comprised of 40 miles of 161 kV transmission lines. Therefore, MRO determined that this violation did not pose a serious or substantial risk to the BPS.	6/18/2007	5/13/2011	$0	Self-Report	RPU performed the following actions to mitigate the violation: 1) scheduled an outage on April 20, 2011 through April 21, 2011 at the substation to upgrade jumpers on two of the four ring bus line bays to parallel 795 ACSR that has a rating of 1828 amps (510 MVA) at 90 degrees C rise, with a 40 degree ambient. The jumpers for the remaining two ring bus line bays were upgraded on May 4, 2011 through May 5, 2011, again using the same parallel 795 ACSR; and 2) RPU revised its Facility Ratings Methodology document to version 3. This revision included more definitions and documentation of the size requirements for RPU substation jumpers.	5/13/2011	6/28/2011	Admits

Attachment A-1

July 29, 2011 Public Spreadsheet - Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	Haywood Electric Membership Corporation (Haywood)	NCR10293	SERC201100761	NOCV	On February 22, 2011, Haywood, as a Load-Serving Entity, self-reported to SERC a violation of CIP-001-1 R1 for failing to have procedures for the recognition of and for making its operating personnel aware of sabotage events on its facilities and multi site sabotage affecting larger portions of the Interconnection.	CIP-001-1	1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Haywood is a minimal size utility of 84 MW serving 25,320 residential and 605 commercial customers with 0.42 miles of transmission lines at 115 kV. Haywood does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS would be recognized and reported by the TO/TOP.	1/16/2009	2/24/2011	$0	Self-Report	Haywood developed a Sabotage Reporting Procedure that: 1. Includes provisions for making operating personnel aware of sabotage events; 2. Provides procedures for communicating information on sabotage events through a Sabotage Reporting Form; 3. Provides personnel with sabotage response guidelines; and 4. Establishes communication contacts and guidelines with law enforcement officials.	2/24/2011	6/3/2011	Admits
SERC	Haywood Electric Membership Corporation (Haywood)	NCR10293	SERC201100764	NOCV	On February 22, 2011, Haywood, as a Load-Serving Entity, self-reported to SERC a violation of CIP-001-1 R2 for failing to have procedures for the communication of information concerning sabotage events to appropriate parties in the Interconnection.	CIP-001-1	2	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Haywood is a minimal size utility of 84 MW serving 25,320 residential and 605 commercial customers with 0.42 miles of transmission lines at 115 kV. Haywood does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS would be recognized and reported by the TO/TOP.	1/16/2009	7/17/2009	$0	Self-Report	Haywood developed a Sabotage Reporting Procedure that: 1. Includes provisions for making operating personnel aware of sabotage events; 2. Provides procedures for communicating information on sabotage events through a Sabotage Reporting Form; 3. Provides personnel with sabotage response guidelines; and 4. Establishes communication contacts and guidelines with law enforcement officials.	2/24/2011	6/3/2011	Admits
SERC	Haywood Electric Membership Corporation (Haywood)	NCR10293	SERC201100763	NOCV	On February 22, 2011, Haywood, as a Load-Serving Entity, self-reported to SERC a violation of CIP-001-1 R3 for failing to provide its operating personnel with sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events.	CIP-001-1	3	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Haywood is a minimal size utility of 84 MW serving 25,320 residential and 605 commercial customers with 0.42 miles of transmission lines at 115 kV. Haywood does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS would be recognized and reported by the TO/TOP.	1/16/2009	6/2/2010	$0	Self-Report	Haywood developed a Sabotage Reporting Procedure that: 1. Includes provisions for making operating personnel aware of sabotage events; 2. Provides procedures for communicating information on sabotage events through a Sabotage Reporting Form; 3. Provides personnel with sabotage response guidelines; and 4. Establishes communication contacts and guidelines with law enforcement officials.	2/24/2011	6/3/2011	Admits
SERC	Haywood Electric Membership Corporation (Haywood)	NCR10293	SERC201100762	NOCV	On February 22, 2011, Haywood, as a Load-Serving Entity, self-reported to SERC a violation of CIP-001-1 R4 for failing to establish communications contacts with the local Federal Bureau of Investigation and to develop reporting procedures as appropriate to their circumstances.	CIP-001-1	4	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. Haywood is a minimal size utility of 84 MW serving 25,320 residential and 605 commercial customers with 0.42 miles of transmission lines at 115 kV. Haywood does not own or operate any BPS facilities; and 2. The interconnecting Transmission Owner/Transmission Operator (TO/TOP) has procedures pursuant to CIP-001-1 such that sabotage activities directly affecting the BPS would be recognized and reported by the TO/TOP.	1/16/2009	7/17/2009	$0	Self-Report	Haywood developed a Sabotage Reporting Procedure that: 1. Includes provisions for making operating personnel aware of sabotage events; 2. Provides procedures for communicating information on sabotage events through a Sabotage Reporting Form; 3. Provides personnel with sabotage response guidelines; and 4. Establishes communication contacts and guidelines with law enforcement officials.	2/24/2011	6/3/2011	Admits
SERC	Associated Electric Cooperative, Inc. (AECI)	NCR01177	SERC2010000537	NOCV	On May 21, 2010, AECI, as a Generator Owner, self-reported to SERC a violation of FAC-008-1 R1 because AECI's Facility Rating Methodology (FRM) did not include relay protective devices, terminal equipment, and series and shunt compensation devices as required by the Standard.	FAC-008-1	1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system because: 1. AECI's FRM was designed to reflect the most limiting element in the Facility, the generator. 2. While AECI failed to include terminal equipment and series and shunt compensation devices in its FRM, AECI has never owned terminal equipment and series and shunt compensation devices.	6/18/07	5/17/10	$0	Self-Report	AECI updated its generator Facility Ratings Methodology document to include relay protective devices, terminal equipment and series and shunt compensation devices.	5/17/10	2/4/11	Admits

Attachment A-1

July 29, 2011 Public Spreadsheet - Administrative Citation Notice of Penalty Spreadsheet

NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	Choctaw Generation Limited Partnership (Choctaw)	NCR10206	SERC201000514	NOCV	On April 1, 2010, Choctaw self-reported to SERC a violation of PRC-005-1 R2 stating that during an internal review of its compliance with NERC standards in March 2010, it determined that complete documentation of the maintenance and testing performed for the Red Hills Plant's Protection System was not available. In the Self-Report, Choctaw stated that test reports from a contractor retained to do testing did not identify the complete scope of the testing performed and did not provide detailed test result sheets for each specific component. The testing contractor provided a letter to Choctaw certifying that it had tested specified relays in March 2007, but acknowledged that documentation of the testing results was not available. Therefore, Choctaw, as a Generator Owner that owns a generation Protection System, is in violation of PRC-005-1 R2 because 101 out of a total of 104 Protection System devices were maintained and tested outside the defined interval or no previous test records were available. From SERC staff's review, it determined that all of Choctaw's Protection System devices, with the exception of the batteries, were tested at the time of commissioning in 1999 and 2000. However, Choctaw did not have sufficient documentation that all of the Protection System devices had been tested and maintained within the defined intervals.	PRC-005-1	2	High	Severe	SERC staff determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. The Transmission Owner (TO)/Transmission Operator-owned (TOP) circuit breakers and bus are approximately 75 yards from the generating facility and contain a dedicated protection scheme that operates independently of the Choctaw site. This system is coordinated to separate the Choctaw facility from the system in the event of a fault that cannot be cleared by opening the Choctaw generator breaker; 2. The generators are protected with two independent microprocessor protection systems with directional power and differential current protections. Both relays operate from independent DC sources and dedicated instrument transformers. The microprocessor relay self-test and diagnostic functions are monitored and alarmed to the control room in the event of a relay failure. This alarm function ensures that any abnormality is immediately brought to the attention of the control room operator; 3. The zones of differential protection are overlapped to ensure full coverage of the entire system and back-up protections including breaker fail protection is designed to operate to trip the TO/TOP breakers in the event the generator breaker should fail to open; 4. No issues with the Protection Systems were found during the most recent testing in April 2010, indicating the protective devices should have performed their intended functions if called upon to do so.	6/18/07	6/15/10	$5,000	Self-Report	Choctaw completed the following actions: 1. Tested and maintained all of its Protection System devices in April 2010. 2. Created a scope of work document to provide to all vendors performing maintenance and testing that includes the requirement that all testing records (in electronic and in paper format) be provided by the vendor prior to payment being released. 3. Added the retention of testing records to the Protection System Maintenance and Testing tasks in the Maintenance Management Work Order System.	6/15/10	5/26/11	Admits
SERC	Big Rivers Electric Corporation (BREC)	NCR01180	SERC201000541	NOCV	During an on-site compliance audit on May 26, 2010, SERC staff found BREC, as a Transmission Operator, in violation of EOP-005-1 R2 because BREC did not review and update its restoration plan at least annually or whenever it made changes in the power system network.	EOP-005-1	2	Medium	Moderate	SERC staff determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. BREC had a system restoration plan *System Restoration Plan EC-EOP-1 Rev 5* dated September 29, 2008 and *Rev 6* dated January 18, 2010 that were approved and would have served to provide direction on restoration, in the event of a partial or total shutdown of its system; 2. Changes from *Rev 5* to *Rev 6* of BREC's "System Restoration Plan EC-EOP-1" were not substantive; 3. BREC participated in the Midwest ISO restoration drills in October 2009 using its restoration plan and found no changes were needed after the drill.	9/30/09	1/18/10	$2,000	Audit	BREC performed the following: 1. Implemented an open and shared calendar through the company-wide Outlook Exchange Server, which allows for the viewing of upcoming revision dates and review deadlines of standards related to BREC documents. The calendar is accessible by all employees involved in the approval and review process. Dates will be noted for sixty day, thirty day, and day-of reminders in order to give those involved three opportunities to view and note an upcoming review deadline. 2. A monthly e-mail reminder is sent out by the Compliance Specialist apprising all employees involved in the approval and review process of standards related to BREC documents of upcoming due dates. The e-mail contains three parts: (a) A summary of all standards related to BREC documents within 60 days of their respective due dates; (b) A summary of all standards related to BREC documents within 30 days of their respective due dates; and, (c) A listing of the current documents under review along with their status in the review process.	6/3/10	4/10/11	Admits
WECC	Northern California Power Agency (NCPA)	NCR05278	WECC201002434	NOCV	On September 28, 2010, NCPA self-reported a violation of VAR-002-1.1b R3 to WECC. On September 19, 2010, NCPA's Geysers Unit 4 experienced minor load swings that NCPA personnel initially attributed to the Power System Stabilizer (PSS). Personnel removed the PSS from service at 1715 hours and notified personnel at the dispatch center at 1735 hrs. NCPA personnel did not, however, notify the Transmission Operator of the status change of the PSS until 1748 hours, thirty-three minutes after the PSS was removed from service.	VAR-002-1.1b	3	Medium	Lower	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). During this violation, the notification to the Transmission Operator was made in thirty-three minutes instead of the required thirty minutes. Given that the notification was only three minutes late and that the generator is a small, 54 MW unit, the impact to the BPS is minimal.	9/19/10	9/19/10	$500	Self-Report	NCPA installed SCADA monitoring on the Geysers Unit 4 PSS. All NCPA personnel at its generating facilities were given refresher training on the guidelines for reporting according to Reliability Standards.	12/31/10	4/12/11	Neither Admits nor Denies

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000381	Settlement Agreement	The entity self-reported that its proprietary fiber network did not reside within an identified Physical Security Perimeter using completely enclosed "six wall" border as required by CIP-006-1 R1.1. The entity did not submit any technical feasibility exceptions (TFEs) and did not deploy and document alternative measures to control physical access to such Cyber Assets.	CIP-006-1	1.1	Medium	High	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the fiber was and is privately owned by FRCC_URE1 and all data traffic on the fiber belonged to FRCC_URE1. Also, FRCC_URE1 did have circuit monitoring in place to detect physical intrusion of the fiber network.	4/1/2010	7/22/2010	$14,000 (Settlement of FRCC201000381, FRCC201000396, FRCC200900296, FRCC200900134, FRCC200900135)	Self-Report 7/14/10	1. Installed primary encrypted tunnel. 2. Installed firewalls. 3. Submitted TFEs.	1. 6/25/10 2. 7/22/10 3. 7/29/10	1/25/11 (onsite)	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC201000396	Settlement Agreement	The entity failed to document the assessment of a security patch for applicability within thirty calendar days of availability of the patch. Patch applicability assessment was completed in 35 days instead of the required 30 days.	CIP-007-2a	3.1	Lower	Lower	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the applicable patch was delayed by 5 days and was implemented in the appropriate implementation cycle.	7/16/10	7/21/2010	$14,000 (Settlement of FRCC201000381, FRCC201000396, FRCC200900296, FRCC200900134, FRCC200900135)	Self-Report 9/24/10	1. Verified all patches have been evaluated. 2. Created monthly patch evaluation report. 3. Converted monthly patch evaluation report to bi-monthly.	1. 8/16/10 2. 9/15/10 3. 8/1/10	1/25/11 (onsite)	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900296	Settlement Agreement	The entity's documents were insufficient to demonstrate that it had cyber security test procedures (for workstations, databases, and applications) that minimize the adverse effects to existing security controls within its Electronic Security Perimeter. In addition, the entity's evidence was insufficient to demonstrate that it documented all of its test results.	CIP-007-1	1	Medium	Lower	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because system testing was being performed for the functional requirements which included some security controls.	7/1/08	5/29/2009	$14,000 (Settlement of FRCC201000381, FRCC201000396, FRCC200900296, FRCC200900134, FRCC200900135)	Spot-Check 12/04/09	FRCC_URE1 tested its hardware and software assets by running policy reports through its testing software. The test results confirmed that changes to its system configurations did not compromise existing security measures.	5/29/09	1/20/10 (onsite)	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900134	Settlement Agreement	The entity did not maintain sufficient evidence that training was performed within 90 days for 16 employees (out of 288) and 2 contractors (out of 8 contractors).	CIP-004-1	2 (2.1, 2.3)	Medium	Lower	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the identified employees were long-term employees with physical only access, and the contractors were either security guards or trusted vendors who had been vetted for their employment.	7/1/08	1/27/2009	$14,000 (Settlement of FRCC201000381, FRCC201000396, FRCC200900296, FRCC200900134, FRCC200900135)	Self-Report 1/29/09	1. Reviewed records and revocation of access where appropriate. 2. New procedures became effective including a 10-day freeze on granting access rights. 3. New procedures to verify records of training and background checks prior to granting Critical Cyber Asset access and to track ongoing access rights for compliance with CIP requirements were communicated and implemented. 4. Monthly reviews of CCA access privileges. 5. Three months of reviews completed. 6. Six months of reviews completed.	1.1/27/09 2.1/29/09 3. 1/29/09 4.3/10/09 5. 6/16/09 6. 9/8/09	1/25/11 (onsite)	Neither Admits nor Denies
FRCC	FRCC_URE1	NCRXXXXX	FRCC200900135	Settlement Agreement	The entity did not maintain sufficient evidence that Personnel Risk Assessments (PRAs) were performed for 16 employees (out of 288) and 4 contractors (out of 8).	CIP-004-1	3	Medium	Moderate	FRCC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because the identified employees were long-term employees with physical only access, the contractors were either security guards or trusted vendors who had been vetted for their employment. In addition the security guards maintained state level Personnel Risk Assessments.	7/1/08	1/27/2009	$14,000 (Settlement of FRCC201000381, FRCC201000396, FRCC200900296, FRCC200900134, FRCC200900135)	Self-Report 1/29/09	1. Reviewed records and revocation of access where appropriate. 2. New procedures became effective including a 10-day freeze on granting access rights. 3. New procedures to verify records of training and background checks prior to granting Critical Cyber Asset access and to track ongoing access rights for compliance with CIP requirements were communicated and implemented. 4. Monthly reviews of Critical Cyber Asset access privileges were implemented. 5. Three months of reviews completed. 6. Six months of reviews completed.	1.1/27/09 2.1/29/09 3. 1/29/09 4.3/10/09 5. 6/16/09 6. 9/8/09	1/25/11 (onsite)	Neither Admits nor Denies

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
NPCC	NPCC_URE1	NCRXXXXX	NPCC201000214	Settlement Agreement	On October 6, 2010, NPCC_URE1 reviewed access logs associated with a particular firewall (i.e. end point) at its back-up control center for unauthorized access to the back-up control center Electronic Security Perimeter (ESP). During the process of performing the access review on 10/6/10, NPCC_URE1 discovered that a violation of CIP-005-2 R3.2 had occurred as the previous manual access review associated with the firewall in question had occurred on 3/22/10. This amounted to a time span of 197 days and is in excess of the 90 calendar days allowed by R3.2.	CIP-005-2	3.2	Medium	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). The manual historical access review performed by NPCC_URE1 on 10/6/10 did not result in the discovery of any unauthorized attempts at access in the past 197 days to the back-up control center ESP via the firewall in question. Also, the firewall in question connects to a frame relay network and does not allow access to the Internet or the NPCC_URE1 corporate network.	6/21/2010	10/6/2010	$7,500	Self-Report	1. NPCC_URE1 discussed the responsibilities of CIP-005-2 R3.2 with the persons directly responsible for compliance with the requirement to review or otherwise review access logs for attempts at or actual unauthorized accesses at least every 90 calendar days when 24x7 alerting is not technically feasible. 2. NPCC_URE1 initiated an immediate historical review of the access logs of the firewall in question at the back-up control center for unauthorized attempts at access and unauthorized actual access. 3. NPCC_URE1 directed completion of an in-progress capital project to provide continuous (24x7) alerting associated with this and several other firewalls. 4. NPCC_URE1 reviewed with the Network Communication and Planning Department and the Critical National Infrastructure Department their specific assigned responsibilities related to Standards CIP 002 – 009. It was agreed to meet quarterly as a group to review these requirements and report on progress.	12/9/2010	2/10/2011	Neither Admits Nor Denies
NPCC	NPCC_URE2 **NextEra Energy Resources, LLC (NextEra)**	NCRXXXXX	NPCC201000215	Settlement Agreement	NPCC_URE2, as Generator Operator and Generator Owner, did not make its cyber security policy readily available to contractors with access to, or responsibility for Critical Cyber Assets.	CIP-003-1	1.2	Lower	Severe	NPCC determined that the violation of CIP-003-1 R1.2 posed a minimal risk and did not create a serious or substantial risk to the reliability of the bulk power system (BPS) because the contractors successfully completed NPCC_URE2's CIP training. The training included the proper use of Critical Cyber Assets; physical and electronic access controls to Critical Cyber Assets; the proper handling of Critical Cyber Asset information; action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident. In addition the contractors had to have a satisfactory documented Personnel Risk Assessment prior to access being granted	1/1/2010	9/30/2010	$5,000	Self-Report	NPCC_URE2 e-mailed a copy of its cyber security policy to each contractor with remote authorized cyber access. NPCC_URE2 placed a copy of the cyber security policy at a central location of each Critical Asset within the NPCC region and explained on the Physical Security Perimeters' sign-in, sign out log the availability of the cyber security policy. NPCC_URE2 updated the contractor eligibility process to include the process step to send the contractor the cyber security policy and copy the supervisor after the contractor becomes eligible for access. The contractor becomes eligible for access once he/she successfully meets the Personnel Risk Assessment and training requirements.	9/30/2010	4/19/2011	Does Not Contest

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
NPCC	NPCC_URE3	NCRXXXXX	NPCC201100250	NOCV	On January 1, 2010, the control systems for two NPCC_URE3 generating units were added by NPCC_URE3_Parent to the NPCC_URE3 Critical Cyber Asset (CCA) list. There were no technical feasibility exception (TFE) requests made associated with the control systems of either unit. The proper assessment, documentation, and installation of patches associated with both control systems were not performed as per CIP-007-3 R3 between 1/1/10 and 12/1/10. The control systems for both units are not connected to an outside network. The isolated nature of both control systems contributed to the difficulty of installing security patch updates and malware prevention software without the potential of introducing viruses. However, NPCC_URE3 did not make any TFE requests. The technological age of the control systems and inherent vendor support issues added to the difficulties. These difficulties led to a lack of proper assessment, updates, documentation, and installation relating to R3.	CIP-007-3	3	Lower	Lower	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) as the control systems for both units utilized non-routable protocol during the entire timeframe. At no time, were they ever connected to a network. There was no actual impact to the BPS as the operation of both units were never effected due lack of patches performed or anti-virus software installed because a connection to a network was never made.	1/1/2010	12/1/2010	$0	Self-Report	1. On December 1, 2010, upon the completion of an internal assessment, the control systems for both units were removed from the CCA list. 2. On December 16, 2010, NPCC_URE3_Parent hired a full-time Regional CIP Engineer whose job description is to provide CIP guidance to the plant, which will include identifying situations that require TFEs. 3. On 1/20/11, training was completed for appropriate IT personnel on patching and anti-virus requirements associated with CIP-007.	1/20/2011	5/6/2011	Admits
NPCC	NPCC_URE3	NCRXXXXX	NPCC201100251	NOCV	On January 1, 2010, the control systems for NPCC_URE3_Parent's two NPCC_URE3 generating units were added to the NPCC_URE3 Critical Cyber Asset (CCA) list by NPCC_URE3_Parent. There were no technical feasibility exception (TFE) requests made associated with the control systems of either unit. NPCC_URE3 is a wholly owned subsidiary of NPCC_URE3_Parent. The proper assessment, documentation, and installation of patches associated with both control systems were not performed as per CIP-007-3 R3 between 1/1/10 and 12/1/10. The control systems for both units are not connected to an outside network. The isolated nature of both control systems contributed to the difficulty of installing security patch updates and malware prevention software without the potential of introducing viruses. However, NPCC_URE3 did not make any TFE requests. The technological age of the control systems and inherent vendor support issues added to the difficulties. These difficulties led to a lack of proper assessment, updates, documentation, and installation as required by R3.	CIP-007-3	4	Lower	Severe	The violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) as the control systems for both units utilized non-routable protocol during the entire timeframe. At no time, were they ever connected to a network. There was no actual impact to the BPS as the operation of both units were never effected due lack of patches performed or anti-virus software installed because a connection to a network was never made.	1/1/2010	12/1/2010	$0	Self-Report	1. On December 1, 2010, upon the completion of an internal assessment, the control systems for both units were removed from the CCA list. 2. NPCC_URE3_Parent hired a full-time Regional CIP Engineer whose job description is to provide CIP guidance to the plant, which will include assisting appropriate plant personnel in identifying situations that require TFEs. 3. Training was completed for appropriate plant personnel on patching and anti-virus requirements associated with CIP-007.	1/20/2011	5/6/2011	Admits

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
MRO	MRO_URE1	NCRXXXXX	MRO201100248	NOCV	During a CIP Spot-Check of MRO_URE1 conducted July 26, 2010 through August 6, 2010, MRO determined that MRO_URE1 did not have controls in place to ensure that it was notified by its energy management system (EMS) vendor when individuals were terminated from the vendor's employ. MRO_URE1 was notified on June 30, 2010 that a member of the vendor's staff supporting the MRO_URE1 EMS system had voluntarily terminated employment and his access had been revoked. On July 6, 2010 MRO_URE1 terminated this employee's logical access to Critical Cyber Assets and updated its list of personnel with access to Critical Cyber Assets within seven calendar days as required. MRO_URE1 then learned that the vendor's employee had voluntarily terminated employment on May 14, 2010, and the vendor failed to notify MRO_URE1 until June 30, 2010.	CIP-004-1	R4.2	Lower	Moderate	MRO determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because although MRO_URE1 did not revoke the individual's access within seven days of termination of employment, the EMS vendor revoked access to its facilities and revoked the individual's remote logical access to MRO_URE1's EMS system from the vendor's site. In order for the vendor's employee to gain access to MRO_URE1's Critical Cyber Assets, the employee must have access to a secured area, along with an authorized account on a workstation specifically used for supporting the MRO_URE1 EMS system. Without access to either the secure area or the specific workstation, the vendor's employees are not able to gain logical access to the MRO_URE1 EMS system from outside of MRO_URE1's defined Electronic Security Perimeter.	7/1/2008	12/16/2010	$0	Spot-Check	MRO_URE1 began e-mailing its EMS vendor every Monday to verify that the list of people with logical access to the MRO_URE1 EMS had not changed in the past seven days. The EMS vendor developed and implemented a secure web-based portal through which MRO_URE1 is able to access all of the information required by CIP-004-2 R2, R3 and R4. If the vendor's employee is no longer a part of the MRO_URE1 EMS project team, voluntarily leaves the employment of the vendor, or is removed for cause by the vendor, as soon as the vendor revokes access at its site, an automatic e-mail is generated alerting MRO_URE1 personnel to revoke the logical access to the EMS system and update the list of authorized vendor employees. This secure web-based portal became operational on December 16, 2010. MRO_URE1 accesses this secure portal on a weekly basis and compares the list of the vendor's names with its list of vendor personnel with logical access to MRO_URE1's EMS.	12/16/2010	5/12/2011	Admits
MRO	MRO_URE2	NCRXXXXX	MRO201100277	NOCV	During a CIP Spot-Check of MRO_URE2 conducted December 6, 2010 through December 16, 2010, MRO determined that MRO_URE2 failed to update its Cyber Security Incident response plan to reflect a process for updating the plan within thirty calendar days of any changes as required by Reliability Standard CIP-008-2 R1.4. MRO_URE2's Cyber Security Incident response plan stated that updating would occur within 90 days as required by version 1 of the CIP Reliability Standards. The cause of the violation was an oversight during the annual review process.	CIP-008-2	R1	Lower	High	MRO determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the bulk power system (BPS) because although MRO_URE2 failed to update its Cyber Security Incident response plan to reflect the 30 calendar day requirement, MRO_URE2 had a cyber incident response plan in place that: (1) provided procedures to characterize and classify events as reportable Cyber Security Incidents; (2) addressed response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans; (3) provided a process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center; and had a process for ensuring that the Cyber Security Incident response plan is reviewed at least annually. Additionally, to date, MRO_URE2 has not had a Cyber Security Incident which would have required the use of the Cyber Security Incident response plan and supporting documentation.	4/1/2010	12/8/2010	$0	Spot-Check	MRO_URE2 updated its Cyber Security Incident response plan to reflect the 30 calendar day requirement.	12/8/2010	6/7/2011	Admits
SERC	SERC_URE1 **Town of Stantonsburg**	NCRXXXXX	SERC201000716	NOCV	On December 7, 2010, SERC_URE1, as a Load Serving Entity, self-reported to SERC a violation of CIP-002-1 R1 for failing to document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-002-1	1	Medium	Severe	SERC finds that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE1 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in the proposed CIP-002-4; 2. SERC_URE1 performed a review of its assets and determined it did not have any Critical Assets, but it failed to document the RBAM as well as the application of the RBAM as required by the Standard; and 3. SERC_URE1 is a minimal size distribution utility with a peak load of 6 MW which serves 1,095 residential customers and 80 commercial consumers and does not own any BPS facilities. SERC_URE1 is only included on the NERC Compliance Registry because the interconnected Transmission Operator requires it to own and operate an underfrequency load shedding system.	12/31/09	4/19/11	$0	Self-Report	SERC_URE1 developed a procedure establishing a written RBAM that identifies Critical Assets, Critical Cyber Assets (if any), and requires the annual review of its RBAM and list of Critical Assets and Critical Cyber Asset (if any).	4/19/11	5/12/11	Admits

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	SERC_URE1 **Town of Stantonsburg (Stantonsburg)**	NCRXXXXX	SERC201000717	NOCV	On December 7, 2010, SERC_URE1, as a Load Serving Entity, self-reported to SERC a violation of CIP-003-1 R2 for failing to assign a senior manager with overall responsibility and authority for leading and managing the entity's adherence to Standards CIP-002 through CIP-009. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-003-1	2	Lower	Severe	SERC finds that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE1 has no critical assets and does not own or operate any facilities that would meet any of the Critical Asset criteria set forth in CIP-002-4; and 2. SERC_URE1 had a senior manager tasked with the responsibility of approving the risk-based methodology, the list of Critical Assets, and the list of Critical Cyber Assets for the CIP-002 self-certifications however, SERC_URE1 had not formally designated and documented the senior manager with the specificity required by the Standard.	12/31/08	2/7/11	$0	Self-Report	SERC_URE1 developed a formal written document that assigned the utility director as the senior manager with the responsibility for leading and for managing SERC_URE1's adherence to Standards CIP-002 through CIP-009. The document (1) identifies the senior manager by name, title and date of designation; (2) requires that changes to senior management are documented within 30 days; (3) allows the senior manager to delegate specific actions to named delegates; and (4) requires the senior manager to authorize and document any exception from the requirements of the cyber protection policy.	2/7/11	5/12/11	Admits
SERC	SERC_URE2 **Town of Winterville (Winterville)**	NCRXXXXX	SERC201000697	NOCV	On November 23, 2010, SERC_URE2, as a Load Serving Entity, self-reported to SERC a violation of CIP-002-1 R1 for failing to document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-002-1	1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE2 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4; 2. SERC_URE2 performed a review and determined that it did not have any Critical Assets but failed to document its RBAM as well as its application of the RBAM as required by the Standard; and 3. SERC_URE2 is a minimal size distribution utility of 12 MW serving 2600 residential customers and 100 small to medium commercial consumers and meets no criteria for inclusion on the Compliance Registry other than the requirement by its Transmission Operator to own and operate an automatic underfrequency load shedding (UFLS) system.	12/31/09	4/13/11	$0	Self-Report	SERC_URE2 developed a procedure establishing a written RBAM that identifies Critical Assets, Critical Cyber Assets (if any), and requires the annual review of its RBAM and list of Critical Assets and Critical Cyber Assets (if any).	4/13/11	5/24/11	Admits
SERC	SERC_URE2 **Town of Winterville (Winterville)**	NCRXXXXX	SERC201000699	NOCV	On November 23, 2010, SERC_URE2, as a Load Serving Entity, self-reported to SERC a violation of CIP-003-1 R2 for failing to assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-003-1	2	Lower	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE2 is a minimal size distribution utility of only 12 MW and meets no criteria for inclusion on the Compliance Registry other than the requirement by its Transmission Operator to own and operate an automatic underfrequency load shedding (UFLS) system; and 2. SERC_URE2 had a senior manager tasked with the responsibility of approving the risk based methodology, the list of critical assets, and the list of critical cyber assets for the CIP-002 self-certifications; however, SERC_URE2 had not formally designated and documented the senior manager with the specificity required by the Standard.	12/31/08	1/29/11	$0	Self-Report	SERC_URE2 prepared a senior manager designation form that assigned a single manager with overall responsibility and authority for leading and managing SERC_URE2's adherence to CIP-002 through CIP-009. The form (1) identifies the senior manager by name, title and date of designation; (2) requires that changes to senior management are documented within 30 days; (3) allows the senior manager to delegate specific actions to named delegates; and (4) requires the senior manager to authorize and document any exception from the requirements of the cyber protection policy.	1/29/11	3/15/11	Admits
SERC	SERC_URE3 **Town of Sharpsburg (Sharpsburg)**	NCRXXXXX	SERC201000719	Notice of Confirmed Violation	On December 7, 2010, SERC_URE3, as a Load Serving Entity, self-reported to SERC a violation of CIP-002-1 R1 for failing to document a risk-based assessment methodology (RBAM) to use to identify its Critical Assets. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-002-1	1	Medium	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE3 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in the proposed CIP-002-4; 2. SERC_URE3 performed a review and determined that it did not have any Critical Assets, but failed to document its RBAM as well as the application of the RBAM as required by the Standard; and 3. SERC_URE3 is a minimal size distribution utility with a peak load of 5 MW which serves 1,132 residential customers and 136 commercial consumers and is included on the NERC Compliance Registry solely because its interconnected Transmission Operator requires it to own and operate an underfrequency load shedding system.	12/31/09	4/22/11	$0	Self-Report	SERC_URE3 developed a procedure establishing a written RBAM that identifies Critical Assets, Critical Cyber Assets (if any), and requires the annual review of its RBAM and list of Critical Assets and Critical Cyber Assets (if any).	4/22/11	5/24/11	Admits

Attachment A-2 - July 29, 2011 Public Spreadsheet -
PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date	Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits," "Neither Admits nor Denies" or "Does Not Contest"
SERC	SERC_URE3 **Town of Sharpsburg (Sharpsburg)**	NCRXXXXX	SERC201000721	NOCV	On December 7, 2010, SERC_URE3, as a Load Serving Entity, self-reported to SERC a violation of CIP-003-1 R2 for failing to assign a senior manager with overall responsibility and authority for leading and managing the entity's implementation of, and adherence to, Standards CIP-002 through CIP-009. This violation also applies to Version 2 and Version 3 of the Standard since the duration of the violation spans the enforceable dates of each version.	CIP-003-1	2	Lower	Severe	SERC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: 1. SERC_URE3 has no Critical Assets and does not own or operate any facilities that would meet any of the Critical Asset Criteria set forth in CIP-002-4; and 2. SERC_URE3 had a senior manager tasked with the responsibility of approving the risk based methodology, the list of critical assets, and the list of critical cyber assets for the CIP-002 self-certifications; however, SERC_URE3 had not formally designated and documented the senior manager with the specificity required by the Standard.	12/31/08	2/11/11	$0	Self-Report	SERC_URE3 developed a formal written document that assigned the utility director as the senior manager with the responsibility for leading and for managing SERC_URE3's adherence to Standards CIP-002 through CIP-009. The document (1) identifies the senior manager by name, title and date of designation; (2) requires that changes to senior management are documented within 30 days; (3) allows the senior manager to delegate specific actions to named delegates; and (4) requires the senior manager to authorize and document any exception from the requirements of the cyber protection policy.	2/11/11	5/6/11	Admits

Document Content(s)

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NP12-10

See .pdf page 51: GenOn REMA 1, GenOn REMA 2, GenOn REMA 3, and GenOn REMA 4 (collectively, the GenOn Entities), successors in interest to RRI Energy Mid-Atlantic Holdings, LLC (REMA)

December 30, 2011

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

Re: NERC Spreadsheet Notice of Penalty
FERC Docket No. 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 21 Registered Entities[2] listed therein,[3] in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[4]

The Spreadsheet NOP resolves 54 violations[5] of 16 Reliability Standards. In order to be a candidate for inclusion in the Spreadsheet NOP, the violations are those that had a minimal or moderate impact on the reliability of the bulk power system (BPS). In all cases, the NOP sets forth whether the violations have been mitigated, certified by the respective Registered Entities as mitigated, and verified by the Regional Entity as having been mitigated.

---

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

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

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

As discussed below, this Spreadsheet NOP resolves 54 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.

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.

[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).

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)

NERC

Attachment b

Additions to the service list

ATTACHMENT B

NON-PUBLIC - REGISTERED ENTITY SERVICE LIST FOR DECEMBER 2011 SPREADSHEET NOP INFORMATIONAL FILING

MRO REGISTERED ENTITIES

For Midwest Independent Transmission System Operator, Inc. (MISO):

William Phillips*
VP Stds Compliance & Strategy
Midwest Independent Transmission System Operator, Inc.
P.O. Box 4202
Carmel IN 46082-4202
(317) 249-5420
wphillips@misoenergy.org

Rebecca Moore Darrah*
Sr. Stds. Compliance Analyst
Midwest Independent Transmission System Operator, Inc.
P.O. Box 4202
Carmel IN 46082-4202
(317) 249-5630
rmooredarrah@misoenergy.org

Christina V. Bigelow*
Compliance Counsel
Midwest Independent Transmission System Operator, Inc.
P.O. Box 4202
Carmel, IN 46082-4202
(317) 249-5132
cbigelow@midwestiso.org

NPCC REGISTERED ENTITIES

For Mirant Bowline, LLC (Mirant Bowline):

Enrique Carbia*
NERC Compliance Manager
GenOn Energy
1155 Perimeter West
Atlanta, GA 30338
(678) 579-5678
(678) 579-5927 – facsimile
Enrique.carbia@genon.com

James Mason*
NERC Compliance Director
GenOn Energy
1000 Main Street
Houston, TX
(832) 357-7093
james.mason@genon.com

For Niagara Mohawk Power Corporation (NMPC):

Katherine E. (Lovette) Smith*
Legal Counsel
National Grid
1 MetroTech Center, 14th Floor
Brooklyn, NY 11201
(718) 403-3320
(718) 403-2809 – facsimile
Katherine.Lovette@us.ngrid.com

Vicki O'Leary*
Reliability Compliance
NationalGrid
40 Sylvan Road
Waltham, MA 0245
(781) 907-2421
(781) 907-5707 - facsimile
vicki.oleary@us.ngrid.com

For Maine Electric Power Company (MEPCO) and Central Maine Power Company (CMP):

Kevin Howes*
Manager - NERC Compliance
Central Maine Power Company (CMP)
83 Edison Drive, Augusta, ME 04336
207-621-3965
(207) 621-4598 – facsimile
kevin.howes@cmpco.com

Brian Conroy*
Director - Electric Systems Engineering
Central Maine Power Company (CMP)
83 Edison Drive, Augusta, ME 04336
207-626-9594
(207) 623-5908 – facsimile
brian.conroy@cmpco.com

SERC REGISTERED ENTITIES

For Progress Energy Carolinas (PEC):

Caren B. Anders*
Vice President Transmission Operations & Planning
Progress Energy Carolinas, Inc.
100 East Davie Street
TPP 18
Raleigh, NC 27601
(919) 546-7497
(919) 546-7175 – facsimile
Caren.Anders@pgnmail.com

Danielle T. Bennett*
Associate General Counsel
Progress Energy Services Company, LLC
410 S. Wilmington Street
PEB 17B2
Raleigh, NC 27601
(919) 546-5941
(919) 546-3805 – facsimile
Dani.Bennett@pgnmail.com

SPP REGISTERED ENTITIES

For Sunflower Electric Power Corporation (Sunflower):

Corey Linville*
Executive Manager Power Supply
Sunflower Electric Power Corporation
2075 W. St John
Garden City, KS 67846
(620) 277-4517
(620) 272-5413 – facsimile
clinville@sunflower.net

Megan Wagner*
Supervisor Corporate Compliance
Sunflower Electric Power Corporation
2075 W. St John
Garden City, KS 67846
(620) 272-5903
(620) 272-5413 – facsimile
mwagner@sunflower.net

Chad Wasinger*
Corporate Compliance Specialist
Sunflower Electric Power Corporation
2075 W. St John
Garden City, KS 67846
(620) 272-5400
(620) 272-5413 – facsimile
wasinger@sunflower.net

Tara Lightner*
Corporate Compliance Assistant
Sunflower Electric Power Corporation
2075 W. St John
Garden City, KS 67846
(620) 272-5412
(620) 272-5413 – facsimile
tlightner@sunflower.net

Lindsay Shepard*
Executive Manager Corporate Compliance &
Associate General Counsel
Sunflower Electric Power Corporation
301 West 13th
Hays, KS 67601
(785) 623-6618
(785) 623-3395 – facsimile
lshepard@sunflower.net

Mark Calcara*
General Counsel
Sunflower Electric Power Corporation
301 West 13th
Hays, Kansas 67601
(785) 623-3320
(785) 623-3395 – facsimile
mcalcara@sunflower.net

Beth Emery*
Counsel
Husch Blackwell, LLP
755 E. Mulberry, Suite 200
San Antonio, TX 78212
(210) 244-8802
(210) 354-4034 – facsimile
beth.emery@huschblackwell.com

Stuart Lowry*
Chief Executive Officer
Sunflower Electric Power Corporation
301 West 13th
Hays, Kansas 67601
(785) 623-3335
(785) 623-3395 – facsimile
slowry@sunflower.net

Texas RE REGISTERED ENTITIES

For ExxonMobil Refining and Supply Company (ExxonMobil0:

Bri Wingert*
UOPS Section Supervisor / NERC Primary Compliance Contact
ExxonMobil Refining and Supply
3525 Decker Drive
BOP MPU 226
Baytown, TX 77520
(281) 834-6252
(281-834-6770 - facsimile
Bri.a.wingert@exxonmobil.com

Matthew Waters*
Business and Technical Department Manager / NERC CEO
ExxonMobil Refining and Supply
3525 Decker Drive
Adm 313
Baytown, TX 77520
(281) 834-6365
(281) 834-6720 – facsimile
Matthew.o.waters@exxonmobil.com

Austin Carr*
Technical Manager
ExxonMobil Refining and Supply
5000 Bayway Dr.
CAB SE 452
Baytown, TX 77522
281-834-0378
Austin.b.carr@exxonmobil.com

Jontae Reese*
Attorney
ExxonMobil Refining and Supply
5000 Bayway Dr.
CAB E240
Baytown, TX 77522
281-834-0365
281-834-0362 – facsimile
Jontae.s.reese@exxonmobil.com

For Brazos Electric Power Cooperative, Inc. (Brazos):

Shari Heino*
Compliance Manager
Brazos Electric Power Cooperative, Inc.
2404 La Salle Ave.
Waco, TX 76702
(254)750-6295
(254)750-6393 - facsimile
sheino@brazoselectric.com

David Carpenter*
General Counsel's Office
Segrest & Segrest, P.C.
28015 West Hwy. 84
McGregor, Texas 76657
(254)848-2600
(254)848-2700 - facsimile
David.Carpenter@segrestfirm.com

For South Texas Electric Cooperative, Inc. (STEC):

Douglas F. John*
Attorney
John & Hengerer
1730 Rhode Island Avenue, N.W.
Suite 600
Washington, D.C. 20036-3116
(202) 429-8801
(202) 429-8805 – facsimile
djohn@jhenergy.com

Michael Packard*
South Texas Electric Cooperative, Inc.
Farm Road 447
P.O. Box 119
Nursery, TX 77976-0119
(361) 575-6491
No facsimile
mpackard@stec.org

For Luminant Generation Company, LLC (Luminant):

Kevin Phillips*
Director, ERCOT Market Services
500 North Akard Street
Dallas, TX 75201
(214) 875-9341
(214) 875-9480 – facsimile
kevin.phillips@energyfutureholdings.com

WECC REGISTERED ENTITIES

For City of Glendale:

Ramon Z. Abueg*
Assistant General Manager-Electrical Services
City of Glendale
141 N. Glendale Avenue
Level 4
Glendale, CA 91206-4496
(818) 548-3297
rabueg@ci.glendale.ca.us

For Northern California Power Agency (NCPA):

James Pope*
General Manager
Northern California Power Agency
651 Commerce Drive
Roseville, CA 95678-6411
(916)781-4200
jim.pope@ncpa.com

For Public Utility District No. 1 of Chelan County (Chelan):

Chad Bowman*
Director - Transmission and Compliance
Public Utility District No. 1 of Chelan County
P.O. Box 1231
Wenatchee, WA 98807
(509) 661-4605
chad.bowman@chelanpud.org

For Griffith Energy:

Jeremy Bergstrom*
Operations Manager
Griffith Energy, LLC - GRGO
P.O. Box 3519
Kingman, AZ 86402
(928) 718-0102
jbergstrom@griffithpower.com

For AES Alamitos LLC (AES):

Weikko Wirta*
Plant Manager
AES Alamitos, LLC
690 N. Studebaker Rd.
Long Beach, CA 90803
(714) 374-1421
weikko.wirta@aes.com

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-003-1 R1 has a Medium VRF; CIP-003-1 R1.1, R1.2 and R1.3 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-003-1 R1 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-003-1 R1 was in effect from June 18, 2007 until January 27, 2009, when the Medium VRF became effective.

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

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

- CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a Medium VRF; R2.5 and its sub-requirements and R2.6 each have a Lower VRF. When NERC filed VRFs it originally assigned CIP-005-1 R2 and R2.4 Lower VRFs. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRF and on February 2, 2009, the

Commission approved the modified Medium VRF. Therefore, the Lower VRFs for CIP-005-1 R2 and R2.4 were in effect from June 18, 2007 until February 2, 2009 when the Medium VRFs became effective.

- CIP-005-1 R3, R3.1 and R3.2 each have a "Medium" VRF. When NERC filed VRFs it originally assigned CIP-005-1 R3, R3.1 and R3.2 "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-005-1 R3, R3.1 and R3.2 were in effect from June 18, 2007 until February 2, 2009 when the "Medium "VRFs became effective.

- CIP-005-1 R4 and R4.2 each have a "Medium" VRF; CIP-005-1 R4.1 has a "Lower" VRF.

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

- CIP-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.

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

- CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a Lower VRF; R5.1, R5.1.3, R5.2.1 and R5.2.3 each have a Medium VRF. When NERC originally filed VRFs it originally assigned CIP-005-1 R5.1 and R5.3.3 Lower VRFs. The Commission approved the VRFs as filed; however, it directed NERC to submit modifications. NERC submitted the modified Medium VRFs and on August 20, 2009, the Commission approved the modified Medium VRFs. Therefore, the Lower VRFs for CIP-005-1 R5.1 and R5.3.3 were in effect from

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

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

- CIP-007-1 R8 and R8.1 each have a "Lower" VRF; R8.2, R8.3 and R8.4 each have a "Medium" VRF.

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

- When NERC filed VRFs it originally assigned MOD-010-0 R1 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 August 6, 2007, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for MOD-010-0 R1 was in effect from June 18, 2007 until August 6, 2007 when the Medium VRF became effective.

- When NERC filed VRFs it originally assigned MOD-010-0 R2 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 August 6, 2007, the Commission approved the modified Medium VRF. Therefore, the Lower VRF for MOD-010-0 R2 was in effect from June 18, 2007 until August 6, 2007 when the Medium VRF became effective.

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

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

NERC

Attachment d

Notice of Filing

ATTACHMENT D

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation Docket No. NP12-___-000

NOTICE OF FILING
December 30, 2011

Take notice that on December 30, 2011, the North American Electric Reliability Corporation (NERC) filed a Spreadsheet Notice of Penalty regarding twenty-one (21) Registered Entities in seven (7) 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

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Midwest Reliability Organization (MRO)	Midwest Independent Transmission System Operator, Inc. (MISO)	NCR00826	MRO201100272	Settlement Agreement	On September 18, 2007, the MRO region experienced a category four disturbance which included a cascade of multiple lines that form the Minnesota-Wisconsin Stability Interface. The loss of these lines was followed by over frequency generator tripping and under frequency load shedding which ultimately resulted in the formation of system islands. MRO initiated a Compliance Violation Investigation (CVI) on March 3, 2008 and NERC assumed leadership of this CVI on March 5, 2008. On September 14, 2009, NERC issued a Preliminary Notice of Findings and Analysis to MISO detailing a finding of noncompliance with the Standard. The CVI team determined that MISO, as the Reliability Coordinator (RC), failed to provide directives to generators in a clear, concise, and definitive manner; failed to use proper three-way communications; and did not ensure that three-way protocols were followed, as required by the Standard. In the first instance, the directive given by MISO to one entity was unclear when it failed to identify the amount of generation MISO was directing be brought online. MRO determined that the entity used three-way communication in repeating back the directive to MISO and responded appropriately. In the second instance, three-way communication procedure was not followed in the directive given by MISO to another entity. MRO determined that even though the directive from MISO to the second entity was clear and carried out properly by the recipient operator, the three-way communication protocol was not followed. The directives were given during the restoration period and did not contribute to the loss of load.	COM-002-2	R2	Medium	Severe (Note that COM-002-2, R2 did not have an assigned VSL or applicable Levels of Noncompliance on the date of the violation, September 18, 2007. The VSL assignments were approved subsequently.)	MRO determined that MISO's violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because in both instances, MISO's directives were followed and correctly implemented, thereby satisfying the Standard's purpose of ensuring effective communications by operating personnel. Further, the Event Analysis Report recognized that MISO's rapid coordination enabled quick restoration (accomplished in 8 minutes 11 seconds) and stabilization of the BPS in the area for which MISO is the Reliability Coordinator.	9/18/2007	9/18/2007
Northeast Power Coordinating Council, Inc. (NPCC)	Mirant Bowline, LLC (Mirant Bowline)	NCR07145	NPCC200900121	Settlement Agreement	During an October 11, 2009 through October 16, 2009 compliance audit of Mirant Bowline, NPCC discovered a violation of PRC-005-1 R1.1. NPCC determined that Mirant Bowline, as a Generator Owner, did not show maintenance and testing intervals for its current transformer (CT) and voltage or potential transformer (PT) generation Protection System devices. Documents provided to NPCC by Mirant Bowline, of its relay maintenance and testing program for the bulk power system, did not show maintenance and testing intervals for its CT and PT devices. The components of the Protection System include protective relays, associated communication systems, CTs, PTs, station batteries and DC control circuits. The 70 total CTs and PTs comprised fewer than 25% of the 408 applicable Protection System devices.	PRC-005-1	R1; R1.1	High	Lower	NPCC Enforcement determined that the violation posed a moderate but not serious or substantial risk to the reliability to the bulk power system. Although Mirant Bowline could not provide evidence that it verified the integrity of the CT and PT devices by performing testing on these devices periodically or defined testing intervals for these devices as per Mirant Bowline's maintenance document, there were no misoperation events or indication of failing/failed devices during the period. CT and PT testing was completed on April 1, 2010 for units 1 and 2, and all CT and PT devices tested satisfactorily. Also, based on evidence reviewed, no other potential evidence of noncompliance was identified with respect to all other aspects of Mirant Bowline. Mirant Bowline also employs back-up relaying providing backup protection should the primary systems fail.	6/21/2007 (When Mirant Bowline registered for the Generator Owner function.)	2/25/2010 (When Mirant Bowline's maintenance and testing program was enhanced to include maintenance and testing intervals for the CT and PT devices.)
Northeast Power Coordinating Council, Inc. (NPCC)	Mirant Bowline, LLC (Mirant Bowline)	NCR07145	NPCC200900122	Settlement Agreement	During an October 11, 2009 through October 16, 2009 compliance audit of Mirant Bowline, NPCC discovered a violation of PRC-005-1 R2.1 and R2.2. NPCC determined that Mirant Bowline, as a Generator Owner, did not show testing of any of its 70 current transformer (CT) and voltage or potential transformer (PT) devices on its generation Protection System list. This list did show a listing of all protective relays, date last tested, testing interval periodicity and next required test date.	PRC-005-1	R2; R2.1; R2.2	High	Severe	NPCC Enforcement determined that the violation posed a moderate but not serious or substantial risk to the reliability to the bulk power system. Although Mirant Bowline could not provide evidence that it verified the integrity of the CT and PT devices by performing testing on these devices periodically or defined testing intervals for these devices as per Mirant Bowline's maintenance document, there were no misoperation events or indication of failing/failed devices during the period. CT and PT testing was completed on April 1, 2010 for units 1 and 2, and all CT and PT devices tested satisfactorily. Also, based on evidence reviewed, no other potential evidence of noncompliance was identified with respect to all other aspects of Mirant Bowline's relay maintenance and testing program for the requirements of PRC-005-1. Mirant Bowline also employs back-up relaying providing backup protection should the primary systems fail.	6/21/2007 (When Mirant Bowline registered for the Generator Owner function.)	5/3/2011 (Mitigation Plan completion.)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Northeast Power Coordinating Council, Inc. (NPCC)	Niagara Mohawk Power Corporation (NMPC)	NCR07163	NPCC201000177	Settlement Agreement	On April 13, 2010, NPCC conducted a Spot Check of NMPC and discovered a violation of COM-002-2 R2. NPCC determined that NMPC, as a Transmission Operator (TOP), was in violation of the Standard. The NMPC control room operator failed to issue directives in a clear, concise, and definitive manner as required by the Standard. When issuing a directive to perform switching at a substation, the NMPC control room operator did not use the proper communication technique. Further, the NMPC control room operator did not ensure that the recipient of the communication repeated the information back correctly, as required by the Standard. The operator at the substation willingly accepted the switching order and performed the switching without incident.	COM-002-2	R2	Medium	Severe	NPCC determined that this violation posed a moderate risk but not serious or substantial risk to the reliability of the bulk power system (BPS) because the communication at issue was given during a period of restoration of equipment, and therefore took place under normal conditions rather than during a time of high stress, system instability, or system emergency. Additionally, the directive which was given in an improper manner was nonetheless carried out by the recipient in the correct manner and thus did not cause any additional risk. NPCC determined that there was a moderate risk because the switching directives associated with the communication errors could have been performed incorrectly which would have resulted in delays in proper restoration or additional equipment being forced out of service.	6/14/2009 (when the improper communication occurred)	6/14/2009
Reliability*First* Corporation (RFC)	City of Niles Light Department (City of Niles)	NCR02710	RFC201000674	Settlement Agreement	RFC conducted a compliance audit of the City of Niles from October 18, 2010 to October 29, 2010. RFC determined that the City of Niles, as a Distribution Provider (DP), failed to provide the basis for the testing and maintenance interval applicable to its DC control circuitry in its Protection System maintenance and testing program, in violation of PRC-005-1, R1. RFC determined that although the Program required testing and maintenance according to a four-year testing and maintenance interval, the City of Niles did not document the basis for the identified testing and maintenance interval, as required by PRC-005-1, R1. The DC control circuitry represents 2 of 53 Protection System devices.	PRC-005-1	R1	High	Severe (from July 18, 2007 to May 18, 2011); High from May 19, 2011 to June 22, 2011	RFC 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 the risk was mitigated by several factors. First, the City of Niles is a municipal utility with a peak load of 68 MW. Second, the City of Niles represented that it performed testing on its DC control circuitry devices in May 2007 as part of the installation and commissioning testing, although it did not retain records of the testing activity. In addition, the City of Niles completed maintenance and testing on its DC control circuitry on May 25, 2011 and found no problems with the devices. The entity completed this testing approximately four years from May 2007, the time it last tested the devices, which corresponds to the testing interval for DC circuitry now stated in its maintenance and testing program.	9/28/2007(City of Niles was required to comply with this Standard)	06/22/2011 (Mitigation Plan was completed)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Reliability*First* Corporation (RFC)	City of Niles Light Department (City of Niles)	NCR02710	RFC201000675	Settlement Agreement	RFC conducted a compliance audit of the City of Niles from October 18, 2010 to October 29, 2010. RFC determined that the City of Niles, as a Distribution Provider (DP), failed to provide documentation that it implemented its maintenance and testing program as it applied to its DC control circuitry. The City of Niles failed to provide documentation that it maintained and tested its two DC circuitry devices. As a result, the City of Niles failed to provide evidence (a) that it maintained and tested any of its DC control circuitry within the defined intervals of PRC-005-1, R2, and (b) of the date it last maintained and tested its DC control circuitry, as required by the PRC-005-1, R2	PRC-005-1	R2	High	Severe	RFC 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 the risk was mitigated by several factors. First, the City of Niles is a municipal utility with a peak load of 68 MW. Second, the City of Niles represented that it performed testing on its DC control circuitry devices in May 2007 as part of the installation and commissioning testing, although it did not retain records of the testing activity. In addition, the City of Niles completed maintenance and testing on its DC control circuitry on May 25, 2011 and May 27, 2011 and found no problems with the devices. The entity completed this testing approximately four years from May 2007, the time it last tested the devices, which corresponds to the testing interval for DC circuitry now stated in its maintenance and testing program.	9/28/2007(City of Niles was required to comply with this Standard)	5/27/2011 (date completed the maintenance and testing of its DC control circuitry)
Reliability*First* Corporation (Reliability*First*)	Sunbury Generation LP (Sunbury)	NCR06030	RFC201000629	Settlement Agreement	Reliability*First* conducted a compliance audit of Sunbury (Audit) from September 13, 2010 through September 28, 2010, during which Reliability*First* discovered a violation of VAR-002-1 R2. Reliability*First* determined that Sunbury, as a Generator Operator, had failed to maintain its voltage schedule as directed by its Transmission Operator (TOP). PJM Interconnection, LLC (PJM), Sunbury's TOP, provides a default voltage schedule in the *PJM Manual 03* "Transmission Operations" for those operators that do not receive a specific voltage schedule. The 230 kV voltage schedule is 235 kV, plus or minus 4 kV; *PJM Manual 03* also lists a high limit voltage of 242 kV. Sunbury never received a specific voltage schedule from its TOP, and never obtained an exemption from the TOP. Sunbury does not and cannot control the transformers that control the switchyard voltages because they are located in the switchyards and are owned and operated by a different interconnected utility. On July 12, 2010 and August 20, 2010, the 230 kV switchyard at Sunbury exceeded the PJM default voltage schedule. On July 12, 2010 for forty-five minutes, the Sunbury 230 kV switchyard was at 239.5 kV, and on August 20, 2010 for six hours, the Sunbury 230 kV switchyard was above 239 kV. Although Sunbury exceeded the PJM default voltage schedule; it did not exceed the high limit of 242 kV.	VAR-002-1	R2	Medium	Lower	This violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system because at all relevant times, Sunbury cooperated with any voltage or reactive assistance requests received from the Transmission Owner or from the TOP. Sunbury has never received notification from either the Transmission Owner or the TOP that Sunbury failed to follow a directive related to voltage or reactive assistance. In addition, the Transmission Owner also provided a screen shot from its computers that monitor and control the Susquehanna region 230 kV voltages in which Sunbury is located. This screen shot indicates the high limit of 242 kV, which Sunbury did not exceed. Furthermore, the generator Automatic Voltage Regulators (AVRs) are always operated in automatic mode except during startup periods or in case of malfunction or system anomalies. In all cases, the TOP is notified whenever the AVR is switched to manual mode, and then again when it is returned to automatic mode. Sunbury conducted reactive testing on Unit 4 (required by PJM) on September 28, 2010. This testing requires that the generator be operated to its limit of MVAR lag operation for one hour. Subsequently, the generator must be operated to its limit of MVAR lead operation. Since Sunbury does not control or have access to the yard voltages, the voltage data was provided by the Transmission Owner. The voltage data provided by the Transmission Owner shows that there was no voltage change in the 230 kV yard, even though Sunbury operated the generator to both its lead and lag limits.	8/2/2007 (When the Standard became mandatory and enforceable.)	5/4/2011 (Mitigation Plan completion.)
Reliability*First* Corporation (Reliability*First*)	Sunbury Generation LP (Sunbury)	NCR06030	RFC201000630	Settlement Agreement	Reliability*First* conducted a compliance audit of Sunbury (Audit) from September 13, 2010 through September 28, 2010, during which Reliability*First* discovered a violation of FAC-008-1 R1.2.1. Reliability*First* determined that Sunbury, as a Generator Owner, failed to include the Ratings Methodology for its transmission conductors and relay protective devices in its Facility Ratings Methodology. Although Sunbury mentioned transmission conductors as part of its system and equipment, Sunbury failed to specifically mention transmission conductors and separately identify their Rating.	FAC-008-1	R1.2.1	Medium	High	This violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system because Sunbury did mention the transmission conductors in the Facility Ratings Methodology, and had determined the Ratings for those devices throughout the violation duration. Specifying the transmission conductors as a separate circuit element had no impact on the Facility Ratings overall, nor did it change the identification of the most limiting element.	6/18/2007 (When the Standard became mandatory and enforceable.)	11/4/2010 (When Sunbury revised its Facility Ratings Methodology to include transmission conductors.)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Reliability*First* Corporation (Reliability*First*)	Sunbury Generation LP (Sunbury)	NCR06030	RFC201000631	Settlement Agreement	Reliability*First* conducted a compliance audit of Sunbury (Audit) from September 13, 2010 through September 28, 2010, during which Reliability*First* discovered a violation of PRC-005-1 R1. Reliability*First* determined that Sunbury, as a Generator Owner, failed to include all maintenance and testing intervals and their basis as well as summaries of maintenance and testing procedures for all of its Protection System devices in its Protection System maintenance and testing program. Sunbury's *Procedure PRC-005 Transmission and Generation Protection System Maintenance and Testing* program (Program), dated February 8, 2010, failed to include all necessary elements. The Program failed to include maintenance and testing intervals and their basis for all 50 of its voltage and current sensing devices in violation of PRC-005-1 R1.1. In addition, the Program failed to include summaries of maintenance and testing procedures for all voltage and current sensing devices and its eight direct current control circuits in violation of PRC-005-1 R1.2. This violation involved 58 of Sunbury's 108 (55%) Protection System devices.	PRC-005-1	R1	High	Severe	This violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system. Specifically, the risk was mitigated because Sunbury has redundant protection in place. In addition, Sunbury has alarms that sound in both the plant control rooms and the plant control house upon the loss of power or similar malfunction. Additionally, except as noted in these violation descriptions, Sunbury tested its Protection System devices in accordance with their intervals, and all devices were functional and available.	6/18/2007 (When the Standard became mandatory and enforceable.)	10/20/2010 (When Sunbury updated its Protection System maintenance and testing program.)
Reliability*First* Corporation (Reliability*First*)	Sunbury Generation LP (Sunbury)	NCR06030	RFC201000632	Settlement Agreement	Reliability*First* conducted a compliance audit of Sunbury (Audit) from September 13, 2010 through September 28, 2010, during which Reliability*First* discovered a violation of PRC-005-1 R2. Reliability*First* determined that Sunbury, as a Generator Owner, failed to provide evidence that it maintained and tested direct current control circuitry within the defined intervals and failed to identify the dates that it last tested direct current control circuitry. Sunbury failed to test direct current control circuitry within the defined interval, in violation of PRC-005-1 R2.1. In addition, Sunbury failed to identify the dates that it last tested its direct current control circuitry, in violation of PRC-005-1 R2.2. This violation involved all of Sunbury's direct current control circuitry (100%) which constituted eight of Sunbury's 108 (7.4%) Protection System devices.	PRC-005-1	R2; R2.1; R2.2	High	Severe	This violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system. Specifically, the risk was mitigated because Sunbury has redundant protection in place. In addition, Sunbury has alarms that sound in both the plant control rooms and the plant control house upon the loss of power or similar malfunction. Additionally, except as noted in these violation descriptions, Sunbury tested its Protection System devices in accordance with their intervals, and all devices were functional and available.	6/18/2007 (When the Standard became mandatory and enforceable.)	10/20/2010 (When Sunbury updated its Protection System maintenance and testing program.)
SERC	Progress Energy Carolinas (PEC)	NCR01298	SERC200900412	Settlement Agreement	On December 8, 2009, PEC self-reported a violation of PRC-005-1 R1. During an investigation into battery inspection work orders, PEC discovered that it had failed to include the appropriate basis for battery maintenance intervals in its maintenance and testing documentation as required by the Standard. SERC was able to verify that PEC has a documented transmission Protection System maintenance and testing program. In 2008, PEC's Asset Management group made a recommendation to revise the inspection of substation batteries from a six-month interval to a 12-month interval. The revised procedure was scheduled to become effective on August 1, 2009. With the revision, battery inspection and battery maintenance would be performed together on an annual basis. In addition, under the revised procedure, PEC would start conducting battery and battery charger maintenance together in order to streamline and eliminate unnecessarily redundant maintenance activities. PEC's work management group completed the rescheduling of its battery maintenance activities in anticipation of the revised procedures' August 1, 2009 implementation date but its procedure drafting group did not revise the *Substation Equipment Maintenance Schedule* until September 23, 2009, and the battery maintenance procedure until October 26, 2009. SERC determined that PEC, as a Transmission Owner, was in violation of PRC-005-1 R1.1 for failing to include the appropriate basis for battery maintenance intervals in its maintenance and testing documentation, as required by the Standard. There was no PRC-005-1 R2 issue in connection with this December 8, 2009 Self-Report.	PRC-005-1	R1/ R1.1	High	Lower	SERC determined that the PRC-005-1 R1.1 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 revised procedure had been implemented in PEC's work order management system so that performance of battery maintenance and testing would take place according to the authorized intervals. In addition, all battery voltages are continuously monitored. An alarm would activate if an abnormal voltage was detected, resulting in the initiation of maintenance activity.	8/1/2009 (date PEC's work order management system was changed to implement the new intervals without updating its procedures)	1/11/2010 (Mitigation Plan completion)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
SERC	Progress Energy Carolinas (PEC)	NCR01298	SERC200900306	Settlement Agreement	On August 26, 2009, PEC self-reported a violation of PRC-005-1 R2. PEC discovered this violation while performing an inventory of its Protection System assets located within customer-owned facilities. When PEC inventoried the customer-owned Kinston DuPont 115 kV substation on August 20, 2009, it found two Coupling-Capacitor Voltage Transformers (CCVTs) owned by PEC that were not captured in its database. PEC's Protection System maintenance and testing program for these CCVTs required maintenance to be performed by April 1, 2009, which had not occurred. PEC performed the required maintenance on August 20, 2009. PEC performed a comprehensive inventory of its Protection System components associated with PRC-005-1 under its Mitigation Plan. On October 25, 2010, PEC filed another Self-Report explaining that during the inventory, it found a column ground relay that had not been included in its equipment database. PEC's investigation confirmed that the identified column ground relay did not have sufficient documentation to demonstrate that calibrations had been performed within the eight year intervals (+25 %) as required in the maintenance and testing program. The previous test date was July 27, 1998 and therefore, the subsequent testing should have occurred no later than July 27, 2008; however, the required test was not performed until September 2, 2010. SERC reviewed PEC's Self-Report and its procedure along with the associated records and determined that a violation of PRC-005-1 R2.1 had occurred due to PEC's failure to complete the required testing and maintenance of the relay within the assigned interval. On December 9, 2010, PEC self-reported an additional violation that was discovered while performing its Mitigation Plan inventory. PEC identified a battery that should have been re-classified on July 1, 2008, as a Protection System device in its equipment database. PEC's investigation confirmed that the identified battery did not have sufficient documentation to demonstrate that the required maintenance was performed for the six- and 12-month preventative maintenance (PM) (+25%) as required in the maintenance and testing program. The six-month PM should have been performed no later than June 26, 2008, and the twelve-month no later than August 1, 2008, however the required maintenance and testing was not performed until August 13, 2008. SERC reviewed PEC's Self-Report and procedure along with the associated records	PRC-005-1	R2/ R2.1	High	Lower	SERC determined that the PRC-005-1 R2.1 violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because: (1) The CCVTs are designed to protect a customer's delivery station and the tap lines serving the station. The CCVTs provide a back-up protective function for the components of the BPS. The devices that provide primary protection for the BPS were being tested and maintained at the prescribed intervals. In addition, testing and maintenance was performed on the CCVTs although not within the intervals specified in PEC's Protection System maintenance and testing program; (2) PEC has multiple layers of protection built into its system. Its 500 kV lines have redundant fast-tripping line protection systems that covers faults to the breakers. The column ground relay provides back-up protection. On September 2, 2010, testing was performed on the column ground relay and no recalibration was required; and (3) The maintenance and testing on the battery was performed two weeks out of interval. In addition, PEC monitors battery voltages in real time and monitors should trigger under-voltage alarms. This should allow for a timely response to a battery problem if the voltage were to drop below a pre-determined level.	7/1/2008 (date the battery was re-classified as a Protection System device)	9/30/2010 (Mitigation Plan completion)
Texas Reliability Entity, Inc. (Texas RE)	Brazos Electric Power Co Op, Inc. (Brazos)	NCR04016	TRE201100277	Settlement Agreement	On February 21, 2011, Brazos, as a Generator Operator, submitted a Self-Report identifying a violation of IRO-001-1.1 R8. At 05:18 CST on February 2, 2011, Electric Reliability Council of Texas Independent System Operator (ERCOT ISO), its Reliability Coordinator, was experiencing a system emergency (EEA-2a), when it issued the following verbal directive: "Do not take units off-line while ERCOT is in emergency operations unless it is due to a forced outage. Report when online available capacity is at risk due to an adverse circumstance." At 08:09 the same day, while the system emergency was still in effect, Brazos removed Unit 2 of Whitney Dam, a 15 MW hydroelectric resource, from service in order to conserve water for later use. Realizing the mistake, at 08:11, the Brazos operator requested the Whitney Dam operator return Unit 2 to service, but the unit was then subject to a 30-minute operational limitation delay before restart could occur. Unit 2 was returned to service at 08:42. During the course of the above events, ERCOT ISO was not contacted. Accordingly, Texas RE determined that Brazos did not follow a reliability directive issued by the Reliability Coordinator.	IRO-001-1.1	R8	High	High	Texas RE determined this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) due to the 15 MW size of the unit and because Brazos was able to deploy sufficient additional generation from its other available generation resources.	2/2/2011 (When the Reliability Coordinator issued the directive)	2/2/2011 (When Brazos complied with the directive)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Texas Reliability Entity, Inc. (Texas RE)	Brazos Electric Power Co Op, Inc. (Brazos)	NCR04016	TRE201100278	Settlement Agreement	On February 21, 2011, Brazos, as a Generator Operator, submitted a Self-Report identifying a violation of TOP-001-1 R3. At 05:18 CST on February 2, 2011, Electric Reliability Council of Texas Independent System Operator (ERCOT ISO), its Reliability Coordinator, was experiencing a system emergency (EEA-2a), when it issued the following verbal directive: "Do not take units off-line while ERCOT is in emergency operations unless it is due to a forced outage. Report when online available capacity is at risk due to an adverse circumstance." At 08:09 the same day, while the system emergency was still in effect, Brazos removed Unit 2 of Whitney Dam, a 15 MW hydroelectric resource, from service in order to conserve water for later use. Realizing the mistake, at 08:11, the Brazos operator requested the Whitney Dam operator return Unit 2 to service, but the unit was then subject to a 30-minute operational limitation delay before restart could occur. Unit 2 was returned to service at 08:42. During the course of the above events, ERCOT ISO was not contacted. Accordingly, Texas RE determined that Brazos did not follow a reliability directive issued by the Reliability Coordinator.	TOP-001-1	R3	High	Severe	Texas RE determined this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) due to the 15 MW size of the unit and because Brazos was able to deploy sufficient additional generation from its other available generation resources.	2/2/2011 (When the Reliability Coordinator issued the directive)	2/2/2011 (When Brazos complied with the directive)
Texas Reliability Entity, Inc. (Texas RE)	ExxonMobil Refining and Supply Company (ExxonMobil)	NCR04058	TRE201000124	Settlement Agreement	On May 18, 2010, after receiving notices from Texas RE of an upcoming compliance audit, ExxonMobil submitted a Self-Report to Texas RE concerning a violation of PRC-005-1 R2. The Self-Report described a failure to perform maintenance and testing on station batteries, protective relays, and current and potential transformers with the defined intervals of ExxonMobil's Protection System Maintenance and Testing Program (Program) and failure to provide adequate documentation of maintenance and test results as required by the Program. Texas RE determined that ExxonMobil, as a Generator Owner, missed quarterly testing on battery pilot cell tests, missed the annual battery system load tests and certain 5-year load tests that were required under ExxonMobil's battery maintenance and testing program. ExxonMobil missed testing some relays under its two year maintenance and testing cycle for its protective relays. ExxonMobil also missed some of its annual load check tests for current and potential transformers. 403 or 71% of ExxonMobil's 569 devices were affected.	PRC-005-1	R2	High	High	This violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because although there is a risk of protection system failure or misoperation due to the lack of proper maintenance and calibration of the protective relays and battery systems, Texas RE determined that if the facility experienced an issue, it would be isolated to ExxonMobil's facility. Furthermore, redundant relaying schemes were in place. In addition, the facility at issue is relatively small, providing the BPS with a net of 50 MW capacity operating at approximately 20% capacity factor.	6/28/2007 (date ExxonMobil was registered on the Compliance Registry)	7/15/2011 (Mitigation Plan completion)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Texas Reliability Entity, Inc. (Texas RE)	ExxonMobil Refining and Supply Company (ExxonMobil)	NCR04058	TRE201000123	Settlement Agreement	On May 18, 2010, after receiving notices from Texas RE of an upcoming compliance audit, ExxonMobil submitted a Self-Report to Texas RE concerning a violation of CIP-001-1 R2. The Self-Report described ExxonMobil's failure to include consistent communications procedures in its sabotage reporting guidelines. Texas RE determined that ExxonMobil, as a Generator Operator, did not have a sabotage procedure sufficient to show compliance with the Standard. An ExxonMobil Baytown Complex Emergency Procedure (Procedure) was created in April 2008 to directly address sabotage events that would impact the bulk electric grid. The sabotage procedure did not consistently contain provisions for the communication of information concerning sabotage events to ERCOT Independent System Operator. Texas RE determined that the Procedure was not sufficient as a stand-alone document to demonstrate compliance, as it included multiple procedures concerning various types of sabotage that could impact the electric grid.	CIP-001-1	R2	Medium	High	This violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because ExxonMobil operators were aware of the requirement to contact ERCOT ISO as an operating practice. Certain, but not all, ExxonMobil sabotage procedures specify ERCOT ISO as a party to contact in the event of sabotage. Texas RE determined that this violation was principally documentation-related.	6/28/2007 (date ExxonMobil was registered on the Compliance Registry	1/12/2011 (Mitigation Plan completion)
Texas Reliability Entity, Inc. (Texas RE)	Luminant Generation Company, LLC (Luminant)	NCR10219	TRE201000273	Settlement Agreement	On September 2, 2010, Luminant submitted a Self-Report identifying a violation of PRC-005-1 R2. Luminant, as a Generator Owner, failed to perform maintenance and testing on some of its protection system devices within the stated intervals required by its Protection System Maintenance and Testing Program (Program). Out of 1,068 protection system devices, tests for 76 devices (7.12% of total devices) comprising some relays and instrument transformers were completed outside the documented test intervals (three-year periodicity). These 76 protection system devices were not identified and included in Luminant's Program. All of these relays and sets of current transformers are related to generator breaker failure protection in the switchyard which was common to both the generating units and the Transmission Owner until 2001, when the ownership of the switchyard devices was segregated. After ownership transfer, Luminant did not consistently include the generator breaker failure and bus differential devices in its program which led to these devices not being identified. Prior to 2001, all these devices were maintained by the Transmission Owner. Overall, current transformers and potential transformers were included as a protection category in the maintenance and testing program, only the specific devices mentioned in this violation were left out of the program.	PRC-005-1	R2	Lower	Lower	The potential risk was considered a moderate risk but not a serious or substantial risk to the bulk power system. Most of the relays and associated CTs which were not timely tested are micro-processor based devices and self-monitored. NERC and industry maintenance standards recommend testing such devices anytime between five years and 12 years. Luminant has three-year testing intervals. Moreover, all devices were properly maintained and tested prior to September 2001 by the transmission provider.	1/31/2008 (date Luminant registered with NERC registry)	11/16/2011 (the date the Mitigation Plan was completed)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Texas Reliability Entity, Inc. (Texas RE)	Big Brown Power Company, LLC (Big Brown)	NCR10217	TRE201000272	Settlement Agreement	On September 2, 2010, Big Brown submitted a Self-Report identifying a violation of PRC-005-1 R2. Big Brown, as a Generator Owner, failed to perform maintenance and testing on some of its protection system devices within the stated intervals required by its Protection System Maintenance and Testing Program (Program). Out of 58 protection system devices, ten (17.24% of total devices) devices comprising some relays and instrument transformers were completed outside the documented test intervals (three year periodicity). These ten protection system devices were not identified and included in Big Brown's Program. All of these relays and sets of current transformers are related to generator breaker failure protection in the switch yard which was common to both the generating units and the Transmission Owner until 2001, when the ownership of the switchyard devices was segregated. After ownership transfer, Big Brown did not consistently include the generator breaker failure and bus differential devices in its program which led to these devices not being identified. Prior to 2001, all these devices were maintained by the Transmission Owner. Overall, current transformers and potential transformers were included as a protection category in the maintenance and testing program, only the specific devices mentioned in this violation were left out of the program.	PRC-005-1	R2	Lower	Lower	The potential risk was considered a moderate risk but not a serious or substantial risk to the bulk power system. Most of the relays and associated CTs which were not timely tested are micro-processor based devices and self-monitored. NERC and industry maintenance standards recommend testing such devices anytime between five years and 12 years. Big Brown has three-year testing intervals. Moreover, all devices were properly maintained and tested prior to September 2001 by the transmission provider.	1/31/2008 (date Big Brown registered with NERC registry)	11/16/2011 (the date the Mitigation Plan was completed)
Texas Reliability Entity, Inc. (Texas RE)	Tradinghouse Power Company LLC (TPC) (TPC was removed from the NERC registry as a GO effective 1/1/2011)	NCR10220	TRE201000274	Settlement Agreement	On September 2, 2010, TPC submitted a Self-Report identifying a violation of PRC-005-1 R2. TPC , as a Generator Owner, failed to perform maintenance and testing on some of its protection system devices within the stated intervals required by its Protection System Maintenance and Testing Program (Program). Out of 29 protection system devices, eight (27.59% of total devices) devices comprising some relays and instrument transformers were completed outside the documented test intervals (three year periodicity). These eight protection system devices were not identified and included in TPC's Program. All of these relays and sets of current transformers are related to generator breaker failure protection in the switchyard which was common to both the generating units and the Transmission Owner until 2001, when the ownership of the switchyard devices was segregated. After ownership transfer, TPC did not consistently include the generator breaker failure and bus differential devices in its program which led to these devices not being identified. Prior to 2001, all these devices were maintained by the Transmission Owner. On December 31, 2010, Unit 2 of the Tradinghouse Steam Electric Station permanently retired from service. Unit 1 at Tradinghouse was retired in 2009. There are no other generating units at this plant site or assigned to this entity, therefore, TPC no longer has any generation assets and was removed from the NERC registry as a Generator Owner. Overall, current transformers and potential transformers were included as a protection category in the maintenance and testing program, only the specific devices mentioned in this violation were left out of the program.	PRC-005-1	R2	Lower	Moderate	The potential risk was considered a moderate risk but not a serious or substantial risk to the bulk power system. Most of the relays and associated CTs which were not timely tested are micro-processor based devices and self-monitored. NERC and industry maintenance standards recommend testing such devices anytime between five years and 12 years. TPC has three-year testing intervals. Moreover, all devices were properly maintained and tested prior to September 2001 by the transmission provider.	1/31/2008 (date Tradinghouse registered with NERC Registry)	12/31/2010 (the last date TPC's units were operational)

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Western Electricity Coordinating Council (WECC)	AES Alamitos (ALGS)	NCR05002	WECC201102728	Settlement Agreement	On December 8, 2010, WECC notified ALGS that it would be conducting an off-site compliance Audit. On February 18, 2011, ALGS submitted a Self-Report, stating that, as a Generator Owner, it was unable to produce evidence of testing and maintenance within defined intervals for all of its batteries subject to this Standard. During the Audit, WECC's Subject Matter Expert determined that ALGS had a documented Maintenance and Testing Program for its Protection System devices and sampled testing records for 29 devices. ALGS provided evidence of the date the batteries were last tested and maintained but was unable to demonstrate that the testing was performed within the defined intervals specified in its Program for one set of batteries comprised of three batteries. Based on the record and additional information obtained from ALGS, WECC enforcement determined that ALGS could not provide evidence of testing within the intervals defined in its program, in violation of this Standard. The scope of the violation was limited to one set of batteries, which account for less than 25% of ALGS's total batteries.	PRC-005-1	R2.1	High	Lower	WECC determined that this violation did not pose serious or substantial risk and posed a minimal risk to the reliability of the bulk power system because although ALGS failed to test its batteries within the specified intervals, it provided evidence that it tested the devices pursuant to its Plan for Protection Systems, including relays and DC circuitry. Also, ALGS was able to provide evidence of testing for the majority of its batteries subject to PRC-005-1. Further, WECC determined that in the event of a malfunction, ALGS's batteries are equipped with an alarm system designed to immediately alert personnel of any failure or defect.	6/18/2007	3/31/2011
Western Electricity Coordinating Council (WECC)	City of Glendale (GLEN)	NCR05081	WECC201102856	Settlement Agreement	On June 30, 2011, GLEN submitted a Self-Report addressing a violation of the WECC Regional Reliability Standard IRO-STD-006-0, WR1. The purpose of this Standard is the mitigation of transmission overloads due to unscheduled line flow on Qualified Paths. Specifically, on May 11, 2011, GLEN's agent for real time trading and scheduling, ACES Power Marketing LLC (APM), notified GLEN of possible Unscheduled Flow (USF) violations which occurred on October 14, 2010, October 15, 2010, and June 5, 2010. The first instance, event 7617, occurred as a result of the trader failing to respond for one hour, which resulted in 2.2 MW of noncompliance. The second instance, event 7642, occurred when APM responded to a WebSAS alarm and curtailed tag 24096 by 4 MW, providing the necessary relief. Following this response, a purchase was made on tag 24130 which inadvertently pushed the line over its limit, resulting in 0.8 MW of noncompliance. APM attempted to adjust the tag back, which would have resulted in compliance, but WAPA-Lower Colorado (WALC) denied the adjustment due to late submission. The third instance, event 7311, occurred when APM failed to respond to a schedule and tag of 3 MW identified by WebSAS impacting path California-Oregon Intertie Path (COI) that should have been adjusted to 0 MW, resulting in 1.0 MW of noncompliance. At the time of the violation, this Standard applied to GLEN, in its function as a Load-Serving Entity.	IRO-STD-006-0 (Note that on July 1, 2011, this Standard was replaced by IRO-006-WECC-1. The new Standard applies to Balancing Authorities (BA) and Reliability Coordinators (RC). Because GLEN's registered functions do not apply to the new Standard's applicability criterion, the Standard no longer applies to GLEN.)	WR1	N/A	N/A	WECC determined that this violation posed a minimal but not a serious or substantial risk to the reliability of the bulk power system (BPS) because: (1) the transmission operator continued to have the option of curtailing transactions that were directly scheduled on the Qualified Path to reduce loading in the event of an imminent overload; (2) the amount of flow increase on the path was less than 1% of the path ratings; and (3) the violation did not result in an overload of the transmission system. WECC determined that this violation is a "Level 1" noncompliance.	10/14/2010, 10/15/2010, 6/5/2010 (the dates of the three separate events)	10/14/2010, 10/15/2010, 6/5/2010 (the dates of the three separate events)
Western Electric Coordinating Council (WECC)	Griffith Energy, LLC (GRGO)	NCR03052	WECC201002858	Settlement Agreement	On October 21, 2010, GRGO submitted a Self-Report stating that GRGO experienced a problem with its Steam Turbine Generator (STG) on October 12, 2010, and discovered that the Power System Stabilizer (PSS) control for the steam turbine was in an OFF position when it should have been in an ON position. GRGO's plant is comprised of one steam turbine and two combustion turbines. On March 23, 2010, the STG was powered down for a replacement of a bad communications card and then powered up and restored to normal operation. However, because GRGO was not aware that the default position was the OFF position, it did not turn it back ON, and the STG PSS system continued to operate in an OFF position. Based on the record, WECC determined that GRGO, as a Generator Operator, failed to ensure that the STG PSS control system was kept in service at all times in order to provide frequency support to the grid.	VAR-STD-002b-1	WR1	The sanctions for this regional standard are determined based on a level of non-compliance ranging from Level 1 to Level 4	The sanctions for this regional standard are determined based on a level of non-compliance ranging from Level 1 to Level 4	WECC determined that the violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the bulk power system (BPS) because GRGO's two combustion turbines' PSSs were ON during the period of the violation, minimizing the need for GRGO's steam turbine to stabilize the generators. Although the STG PSS system was in the OFF position, the plant as a whole performed in an expected manner and was able to support grid frequency deviations per control design on two separate occasions. In addition, WECC determined that the size of the generator involved - 250 MW steam turbine generator, reduced the risk to the BPS. Also, GRGO investigated all generation data for the period of operation without the STG PSS in service and no abnormalities were noted. GRGO's Transmission Operator, the Western Area Power Administration, showed no abnormalities due to GRGO's STG PSS system being OFF.	3/23/2010	10/12/2010

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Western Electricity Coordinating Council (WECC)	Northern California Power Agency (NCPA)	NCR05278	WECC201102909	Settlement Agreement	On August 19, 2011, NCPA submitted a Self-Report addressing noncompliance with MOD-010-0 R1. According to the Self-Report, during an internal review of standards, NCPA found that, as a Generator Owner, it had not been submitting or checking all data from the regional coordinator Pacific Gas and Electric (PGAE) and had failed to provide complete equipment characteristics and system data and review of data as required. During the investigation, it was discovered that a procedure and process had not been developed or put in place that would ensure accountability and timely submittal and review of data to PGAE.	MOD-010-0	R1	Medium	Lower	WECC found 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 NCPA did not review equipment characteristics and system data prior to submitting the data to PGAE, there had not been any changes to NCPA's system characteristics or load data that would have resulted in a change to its network model. Moreover, the purpose of MOD-010-0 and MOD-012-0 is to establish consistent data requirements, reporting procedures, and system models to be used in the analysis of the reliability of the Interconnected Transmission Systems. WECC relies on data from entities to support the design and operations of the western interconnected power system. The timely and accurate submittal of data is a key factor in preserving system reliability and affects significant economic decisions regarding system expansion and operation. In this case, NCPA's data was timely and accurate and had not changed since previous data submittals to PGAE. NCPA's failure to jointly coordinate reporting and data procedures with PGAE did not affect the reliability of the data submitted. For these reasons, WECC determined this violation posed a minimal risk to the reliability of the BPS.	6/18/2007 (when the Standard became mandatory and enforceable)	11/23/2011
Western Electricity Coordinating Council (WECC)	Northern California Power Agency (NCPA)	NCR05278	WECC201102910	Settlement Agreement	On August 19, 2011, NCPA submitted a Self-Report addressing noncompliance with MOD-010-0 R2. According to the Self-Report, during an internal review of standards, NCPA found that it, as a Generator Owner, failed to implement a formal process that ensures all data is reviewed for accuracy prior to being submitted to the area coordinator. Specifically, NCPA failed to jointly coordinate the development of the data requirements and reporting procedures with Pacific Gas and Electric (PGAE). NCPA's failure to follow a documented procedure for submitting data to PGAE resulted in data being submitted to PGAE prior to NCPA reviewing for accuracy. During the investigation it was discovered that a procedure and process had not been developed or put in place that would ensure accountability and timely submittal and review of data to PGAE.	MOD-010-0	R2	Medium	Lower	WECC found 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 NCPA did not review equipment characteristics and system data prior to submitting the data to PGAE, there had not been any changes to NCPA's system characteristics or load data that would have resulted in a change to its network model. Moreover, the purpose of MOD-010-0 and MOD-012-0 is to establish consistent data requirements, reporting procedures, and system models to be used in the analysis of the reliability of the Interconnected Transmission Systems. WECC relies on data from entities to support the design and operations of the western interconnected power system. The timely and accurate submittal of data is a key factor in preserving system reliability and affects significant economic decisions regarding system expansion and operation. In this case, NCPA's data was timely and accurate and had not changed since previous data submittals to PGAE. NCPA's failure to jointly coordinate reporting and data procedures with PGAE did not affect the reliability of the data submitted. For these reasons, WECC determined this violation posed a minimal risk to the reliability of the BPS.	6/18/2007 (when the Standard became mandatory and enforceable)	11/23/2011
Western Electricity Coordinating Council (WECC)	Northern California Power Agency (NCPA)	NCR05278	WECC201102911	Settlement Agreement	On August 19, 2011, NCPA submitted a Self-Report addressing possible noncompliance with MOD-012-0 R1. According to the Self-Report, during an internal review of standards, NCPA found that it, as a Generator Owner, had not provided dynamic system modeling and simulation data to Pacific Gas and Electric (PGAE), the regional coordinator. During the investigation it was discovered that a procedure and process had not been developed or put in place that would ensure accountability and timely submittal and review of data to PGAE.	MOD-012-0	R1	Medium	Lower	WECC found 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 NCPA did not review equipment characteristics and system data prior to submitting the data to PGAE, there had not been any changes to NCPA's system characteristics or load data that would have resulted in a change to its network model. Moreover, the purpose of MOD-010-0 and MOD-012-0 is to establish consistent data requirements, reporting procedures, and system models to be used in the analysis of the reliability of the Interconnected Transmission Systems. WECC relies on data from entities to support the design and operations of the western interconnected power system. The timely and accurate submittal of data is a key factor in preserving system reliability and affects significant economic decisions regarding system expansion and operation. In this case, NCPA's data was timely and accurate and had not changed since previous data submittals to PGAE. NCPA's failure to jointly coordinate reporting and data procedures with PGAE did not affect the reliability of the data submitted. For these reasons, WECC determined this violation posed a minimal risk to the reliability of the BPS.	6/18/2007 (when the Standard became mandatory and enforceable)	11/23/2011

Attachment A-1

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet
(NON-CIP Violations)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Notice of Confirmed Violation or Settlement Agreement	Description of the Violation	Reliability Standard	Req.	Violation Risk Factor	Violation Severity Level	Risk Assessment	Violation Start Date	Violation End Date
Western Electricity Coordinating Council (WECC)	Northern California Power Agency (NCPA)	NCR05278	WECC201102912	Settlement Agreement	On August 19, 2011, NCPA submitted a Self-Report addressing possible noncompliance with MOD-012-0 R2. According to the Self-Report, during an internal review of standards, NCPA found that it, as a Generator Owner, had not provided complete equipment characteristics and system data and review of data to Pacific Gas and Electric (PGAE), the regional coordinator, for use in the WECC system-wide model. During the investigation it was discovered that a procedure and process had not been developed or put in place that would ensure accountability and timely submittal and review of data to PGAE.	MOD-012-0	R2	Medium	Lower	WECC found 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 NCPA did not review equipment characteristics and system data prior to submitting the data to PGAE, there had not been any changes to NCPA's system characteristics or load data that would have resulted in a change to its network model. Moreover, the purpose of MOD-010-0 and MOD-012-0 is to establish consistent data requirements, reporting procedures, and system models to be used in the analysis of the reliability of the Interconnected Transmission Systems. WECC relies on data from entities to support the design and operations of the western interconnected power system. The timely and accurate submittal of data is a key factor in preserving system reliability and affects significant economic decisions regarding system expansion and operation. In this case, NCPA's data was timely and accurate and had not changed since previous data submittals to PGAE. NCPA's failure to jointly coordinate reporting and data procedures with PGAE did not affect the reliability of the data submitted. For these reasons, WECC determined this violation posed a minimal risk to the reliability of the BPS.	6/18/2007 (when the Standard became mandatory and enforceable)	11/23/2011

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$0	NERC Compliance Violation Investigation	On May 13, 2011, MISO submitted a Mitigation Plan (MIT-07-3708) to MRO to address the violation of COM-002-2 R2. In accordance with the Mitigation Plan, MISO engaged in various mitigation activities, including: (1) provided dedicated communications training to its personnel in two training cycles in 2009 and in every training cycle in 2010; (2) revised its policies and procedures to improve compliance with this Standard, including a script to be used by operators; (3) engaged its Members in development and use of appropriate telephone protocol procedures, training and drills to ensure that communications occur in compliance with the Standard; (4) initiated operator call sampling and incentives; (5) tied the results of such sampling directly to operator performance assessments; and (6) reinforced compliance with this Standard through a slogan contest, all-employee meeting, visual support, and dedicated training.	12/8/2008	5/16/2011	Does not contest	MRO considered the following mitigating factors when determining the penalty amount: (1) MISO has no previous violations of the instant Standard and has other violations in the Reliability*First* region which do not involve the same or similar Standards; (2) MISO has a documented compliance program and culture that are well-defined and well-established through its corporate policy. The MISO Standards Compliance and Strategy department has a staff of eight employees headed by a Compliance Officer; and (3) MISO will conduct by April 1, 2012 two "Communications Forums" focused on control room communications and compliance with this Standard, and intended to promote collaboration and coordination between the entities responsible for complying with this Standard. MRO did not consider the loss of load in the penalty determination because these directives were given during the restoration period after the loss of load. MRO determined that there were no additional mitigating or aggravating factors in determining the penalty amount.
$17,500 (for NPCC200900121 and NPCC200900122)	Compliance Audit	1. Completed testing of CT and PT devices. 2. Revised the Protection System maintenance and testing program to include last testing date and next testing date for CT and PT devices.	5/3/2011	7/28/2011	Neither Admits nor Denies	Mirant Bowline has a documented internal compliance program which was reviewed and considered a neutral factor by NPCC.
$17,500 (for NPCC200900121 and NPCC200900122)	Compliance Audit	1. Completed testing of CT and PT devices. 2. Revised the Protection System maintenance and testing program to include last testing date and next testing date for CT and PT devices.	5/3/2011	7/28/2011	Neither Admits nor Denies	Mirant Bowline has a documented internal compliance program which was reviewed and considered a neutral factor by NPCC. Affiliated entities of Mirant Bowline have prior violations of PRC-005-1 R2.1 which were not considered aggravating factors in penalty determination. The filings: NP09-25-000 (Mirant Mid-Atlantic LLC), NP-10-2-000 (Mirant Potomac River, LLC), NP10-65-000 (Mirant Delta, LLC) and NP11-88-000 (Mirant Potrero, LLC), all include prior PRC-005-1 R2.1 violations by affiliates of Mirant Bowline. These prior violations were not considered aggravating factors because the conduct involved in the instant violation was not repetitive of the prior affiliates' conduct. In addition, there was nothing in the record to suggest that broader corporate issues were implicated.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$25,000	Spot Check	On November 23, 2010, NMPC submitted a Mitigation Plan to address the violation of COM-002-2 R2. In accordance with the Mitigation Plan: (1) NMPC's Transmission Control Center management team began random auditing of three-part communications of Security and System Operator communications. An audit form was developed and random tapes of communications were reviewed and discussed with the operator. The operators are made aware of communication technique expectations during these audits; (2) NMPC performed enhanced internal refresher training during Cycle 3 training in June 2010. Material covered included the COM-002-2 Reliability Standard, the NYISO Communication Running Order, and featured an audit of random communication by all of the class participants; (3) NMPC participated in the NYISO Fall 2010 System Operator Training Seminar, which featured refresher training on COM-002-2 in addition to an exercise in three-part communications at the NYISO Training Center; and (4) NMPC instituted a greater emphasis on three-part communication in all continuing operator training.	12/3/2010	3/11/2011	Neither Admits nor Denies	NPCC considered NMPC's Internal Compliance Program, which was in place at the time of the violation, to be a mitigating factor when determining the penalty amount. Specifically, NPCC considered that NMPC's ICP exists with sufficient Senior Leadership involvement; the ICP describes the annual training program related to compliance; NMPC reviews the ICP program activities regularly; NMPC keeps up to date with NERC/NPCC activities; and NMPC provides ample communication of the company's commitment and expectations of employees.
$4000 (for RFC201000674 and RFC201000675)	Audit	On June 24, 2011, the City of Niles submitted as complete Mitigation Plan (MIT-07-3956) to address the violations of PRC-005-1 R1 and R2. In accordance with the Mitigation Plan, the City of Niles: (1) Revised its Program on June 22, 2011 to include the basis for the four-year testing and maintenance interval for its DC control circuitry; and (2) Performed all outstanding maintenance and testing on its DC control circuitry in accordance with the updated Plan.	6/22/2011	8/26/2011	Neither admits nor denies	RFC determined that there were no aggravating or mitigating factors in determining the penalty amount. RFC stated the City of Niles did not have a formal Internal Compliance Program (ICP).

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$4000 (for RFC201000674 and RFC201000675)	Audit	On June 24, 2011, the City of Niles submitted as complete Mitigation Plan (MIT-07-3956) to address the violations of PRC-005-1 R1 and R2. In accordance with the Mitigation Plan, the City of Niles: (1) Revised its Program on June 22, 2011 to include the basis for the four-year testing and maintenance interval for its DC control circuitry; and (2) Performed all outstanding maintenance and testing on its DC control circuitry in accordance with the updated Plan.	6/22/2011	8/26/2011	Neither admits nor denies	RFC determined that there were no aggravating or mitigating factors in determining the penalty amount. RFC stated the City of Niles did not have a formal Internal Compliance Program (ICP).
$20,000 (for RFC201000629, RFC201000630, RFC201000631, and RFC201000632)	Compliance Audit	1. Sunbury conducted a conference call between Sunbury and the other interconnected utility to discuss voltage control capability; 2. Sunbury contacted PJM to discuss the voltage schedule issue to determine feasibility or possible exclusions; 3. The other interconnected utility conducted a system study to determine suitable voltage control based upon Sunbury maintaining low side generator step-up (GSU) voltage/reactive; 4. The information was submitted to PJM for approval; 5. Sunbury installed metering as necessary; 6. PJM reviewed the study and commented; and 7. PJM issued a voltage directive to Sunbury.	7/6/2011	12/28/2011	Neither Admits nor Denies	Due to extenuating circumstances associated with the violation of VAR-002-1 R2, there is no monetary penalty associated with the violation of VAR-002-1 R2. These included Sunbury never receiving a specific voltage schedule from its TOP, and never obtaining an exemption from the TOP, as well as the fact that Sunbury does not and cannot control the transformers that control the switch yard voltages. Reliability*First* considered Sunbury's compliance program as a mitigating factor in the penalty determination. Sunbury's primary compliance contact reports to the vice president of operations, and its internal compliance program is independent from departments having compliance obligations to the Reliability Standards. In addition, Sunbury reviews the Standards and revises its internal compliance program accordingly. Sunbury also ensures that its compliance staff attends workshops and other available training courses regarding compliance with the Standards.
$20,000 (for RFC201000629, RFC201000630, RFC201000631, and RFC201000632)	Compliance Audit	1. Sunbury revised its Facility Ratings Methodology to specify transmission conductors as a separate element included in the Facility Ratings; and 2. Sunbury also revised its Facility Rating Methodology spreadsheet to include the transmission conductors from the main unit transformers to the generator bay.	11/4/2010	2/15/2011	Neither Admits nor Denies	Reliability*First* considered Sunbury's compliance program as a mitigating factor in the penalty determination. Sunbury's primary compliance contact reports to the vice president of operations, and its internal compliance program is independent from departments having compliance obligations to the Reliability Standards. In addition, Sunbury reviews the Standards and revises its internal compliance program accordingly. Sunbury also ensures that its compliance staff attends workshops and other available training courses regarding compliance with the Standards.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$20,000 (for RFC201000629, RFC201000630, RFC201000631, and RFC201000632)	Compliance Audit	1. Sunbury revised its Program to clarify battery maintenance and testing intervals, and that the maintenance and testing interval listed in the Program applies to all generator Protection System devices; and 2. The revised Program also includes summaries of maintenance and testing procedures for all Protection System devices.	12/3/2010	3/10/2011	Neither Admits nor Denies	Reliability*First* considered Sunbury's compliance program as a mitigating factor in the penalty determination. Sunbury's primary compliance contact reports to the vice president of operations, and its internal compliance program is independent from departments having compliance obligations to the Reliability Standards. In addition, Sunbury reviews the Standards and revises its internal compliance program accordingly. Sunbury also ensures that its compliance staff attends workshops and other available training courses regarding compliance with the Standards.
$20,000 (for RFC201000629, RFC201000630, RFC201000631, and RFC201000632)	Compliance Audit	Sunbury completed all delayed maintenance and testing on direct current control circuitry and began recording the test dates of those devices.	12/3/2010	3/10/2011	Neither Admits nor Denies	Reliability*First* considered Sunbury's compliance program as a mitigating factor in the penalty determination. Sunbury's primary compliance contact reports to the vice president of operations, and its internal compliance program is independent from departments having compliance obligations to the Reliability Standards. In addition, Sunbury reviews the Standards and revises its internal compliance program accordingly. Sunbury also ensures that its compliance staff attends workshops and other available training courses regarding compliance with the Standards.
$12,000 (For SERC200900306, and SERC200900412)	Self-Report	To correct the violation of PRC-005-1 R1.1 and to prevent a recurrence of the violation, PEC performed the following: 1. Developed a specific basis procedure for battery and battery charger maintenance; 2. Revised its Protection Basis Document, which provides the basis for all time-directed preventative maintenance applied to Transmission, Distribution, and Generation Protective Systems on October 26, 2009; 3. Revised the Transmission Maintenance Program Policy to require the group that implements the work management system not to release or modify work orders until they have verified that the procedures governing the work orders have been approved; and 4. Developed check points in a Functional Support Work Scope Document that must be completed by the work management group prior to releasing or modifying work orders. The checklist requires that the procedure's effective date be recorded and verified prior to the release or modification of a work order.	1/11/2010	8/10/2010	Admits	Based on PEC's September 20, 2010 responses to SERC's Compliance Culture Questionnaire, Progress Energy's (PEC's parent company) documented compliance program was initially approved on December 13, 2007, and was developed to formally document and drive existing compliance business practices. PEC's compliance program is disseminated to all organizations within PEC that must comply with NERC Standards. The existence of PEC's compliance program was a mitigating factor in determining the penalty. Progress Energy's compliance program is prepared for and approved by Progress Energy's ERO Steering Committee. The ERO Steering Committee is comprised of officers of PEC and Progress Energy Florida and is chaired by the ERO Compliance Officer, who is Progress Energy's Executive Vice President – General Counsel and Corporate Secretary. The ERO Compliance Officer is independent of all PEC organizations that must comply with NERC Standards. The ERO Compliance Officer reports directly to the Chairman/President/CEO and has direct access to the Board of Directors. Company Officers participate in bi-monthly ERO Steering Committee meetings and compliance initiatives within their respective departments.

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$12,000 (For SERC200900306, and SERC200900412)	Self-Report	To correct the violation of PRC-005-1 R2.1 and to prevent a recurrence of the violation, PEC completed the following actions detailed in its Mitigation Plan: 1. Maintenance was performed on the two 115 kV CCVTs the same day that the location was field-verified; 2. PEC's equipment database was corrected to properly show the two CCVTs as located at the Kinston DuPont 115 kV Substation; 3. PEC performed an inventory of its NERC Protection System assets associated with its PRC-005 Protection System equipment. The inventory included verification of the assets within PEC's equipment database, a physical survey of the Protection System assets at PEC substations, including those with customer-owned equipment, as well as a reconciliation of the physical survey results with the PEC equipment database; and 4. PEC reviewed the equipment database process for improvements and re-emphasized the process through training and leadership with emphasis on the necessity of an accurate equipment database for NERC Protection System maintenance. The training targeted Engineering, Maintenance and Construction personnel and covered PEC's NERC Protection System maintenance & testing program, evidence requirements, the equipment database, and the Equipment Change Request process.	9/30/2010	2/14/2010	Admits	Based on PEC's September 20, 2010 responses to SERC's Compliance Culture Questionnaire, Progress Energy's (parent company) documented compliance program was initially approved on December 13, 2007, and was developed to formally document and drive existing compliance business practices. PEC's compliance program is disseminated to all organizations within PEC that must comply with NERC Standards. The existence of PEC's compliance program was a mitigating factor in determining the penalty. Progress Energy's compliance program is prepared for and approved by Progress Energy's ERO Steering Committee. The ERO Steering Committee is comprised of officers of PEC and Progress Energy Florida and is chaired by the ERO Compliance Officer, who is Progress Energy's Executive Vice President – General Counsel and Corporate Secretary. The ERO Compliance Officer is independent of all PEC organizations that must comply with NERC Standards. The ERO Compliance Officer reports directly to the Chairman/President/CEO and has direct access to the Board of Directors. Company Officers participate in bi-monthly ERO Steering Committee meetings and compliance initiatives within their respective departments.
$8,500 (for TRE201100277 and TRE201100278)	Self-Report	Brazos implemented its mitigation process which emphasizes and clarifies to the Qualified Scheduling Entity (QSE) control room operators and supervisors the required actions in the event of an ERCOT ISO directive. The following two parts reflect the key mitigation activities to this event: 1. Retraining of all QSE control room operators and supervisors to reemphasize their duty and the policy of Brazos to comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. In a meeting of QSE control room operators and supervisors which took place on February 22, 2011, the training was conducted emphasizing the critical nature of following all reliability directives. The importance of complying with Reliability Coordinator directives was reinforced by the manager of market operations and the vice president - power supply and generation at this same meeting. 2. Disciplinary action has been administered to the QSE resource operator on duty and his supervisor in accordance with the Brazos compliance plan dated September 29, 2010, Section D.3, Item 8.B.ii., which institutes "disciplinary action up to and including termination." The resource operator on duty and the market operations specialist received a written reprimand for failing to follow Brazos' procedures. The QSE resource supervisor and manager of market operations also received a written instruction to retrain staff.	4/25/2011	10/4/2011	Neither Admits nor Denies	Brazos' compliance program, in effect at the time of the violation, was considered a mitigating factor in the determination of the penalty amount. Brazos has a named compliance manager with the responsibility to oversee the development, implementation and maintenance of the compliance plan. The compliance manager has direct access to the CEO and/or the Brazos board of directors. Brazos regularly reviews and modifies its internal compliance program on an annual basis. The compliance manager also regularly conducts a compliance awareness program and compliance training program. The compliance training program is included in the compliance plan. Brazos senior management fully supports the compliance program and allocates adequate resources, including outsourcing, self-audits and budgets as well as establishing the necessary positions and associated responsibilities to ensure compliance. Brazos states that on an annual basis it conducts internal audits and reviews its compliance plan.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$8,500 (for TRE201100277 and TRE201100278)	Self-Report	Brazos implemented its mitigation process which emphasizes and clarifies to the Qualified Scheduling Entity (QSE) control room operators and supervisors the required actions in the event of an ERCOT ISO directive. The following two parts reflect the key mitigation activities to this event: 1. Retraining of all QSE control room operators and supervisors to reemphasize their duty and the policy of Brazos to comply with Reliability Coordinator directives unless such actions would violate safety, equipment, or regulatory or statutory requirements. In a meeting of QSE control room operators and supervisors which took place on February 22, 2011, the training was conducted emphasizing the critical nature of following all reliability directives. The importance of complying with Reliability Coordinator directives was reinforced by the manager of market operations and the vice president - power supply and generation at this same meeting. 2. Disciplinary action has been administered to the QSE resource operator on duty and his supervisor in accordance with the Brazos compliance plan dated September 29, 2010, Section D.3, Item 8.B.ii., which institutes "disciplinary action up to and including termination." The resource operator on duty and the market operations specialist received a written reprimand for failing to follow Brazos' procedures. The QSE resource supervisor and manager of market operations also received a written instruction to retrain staff.	4/25/2011	10/4/2011	Neither Admits nor Denies	Brazos' compliance program, in effect at the time of the violation, was considered a mitigating factor in the determination of the penalty amount. Brazos has a named compliance manager with the responsibility to oversee the development, implementation and maintenance of the compliance plan. The compliance manager has direct access to the CEO and/or the Brazos board of directors. Brazos regularly reviews and modifies its internal compliance program on an annual basis. The compliance manager also regularly conducts a compliance awareness program and compliance training program. The compliance training program is included in the compliance plan. Brazos senior management fully supports the compliance program and allocates adequate resources, including outsourcing, self-audits and budgets as well as establishing the necessary positions and associated responsibilities to ensure compliance. Brazos states that on an annual basis it conducts internal audits and reviews its compliance plan.
$13,000 (for TRE201000124 and TRE201000123)	Audit	• ExxonMobil provided all available missing maintenance records for Protection Systems devices to Texas RE. • ExxonMobil discussed TRE's Audit findings with its maintenance personnel, and provided refresher training in the proper use of its scheduling/tracking and record retention systems. • ExxonMobil reviewed its maintenance and testing procedures for its Protection Systems devices, and made modifications to include steps for record retention. • ExxonMobil completed all outstanding maintenance and testing for its Protection Systems devices.	7/15/2011	7/20/2011	Neither Admits nor Denies	Texas RE received the Self-Report on May 18, 2010, after Texas RE sent an Audit notification to ExxonMobil. The Audit concluded July 21, 2010, and is the date the violations were deemed to have been discovered by Texas RE. A Settlement Agreement covering several violations, including a violation of PRC-005-1 R2 for ExxonMobil Oil Corporation - Beaumont Refinery (ExxonMobil BR) (NCR01239), an affiliate of ExxonMobil in the SERC Region, (NOC-428) filed with FERC under NP10-90-000 on March 31, 2010. On April 30, 2010, FERC issued an order stating it would not engage in further review of the Notice of Penalty. Texas RE determined that ExxonMobil BR's previous violation of PRC-005-1 R2 in NOC-428 constituted a prior violation that should be considered an aggravating factor in the penalty determination. While ExxonMobil has multiple documented operating and maintenance procedures in place to ensure NERC compliance, Texas RE did not consider ExxonMobil's compliance program as a mitigating factor in determining the penalty.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$13,000 (for TRE201000124 and TRE201000123)	Audit	ExxonMobil included ERCOT ISO in the contact lists for the following emergency procedures: Bomb Threat, Suspicious Package, Suspicious Powder, and Unauthorized Intruder.	1/12/2011	7/20/2011	Neither Admits nor Denies	Texas RE received the Self-Report on May 18, 2010, after Texas RE sent an Audit notification to ExxonMobil. The Audit concluded July 21, 2010, and is the date the violations were deemed to have been discovered by Texas RE. While ExxonMobil has multiple documented operating and maintenance procedures in place to ensure NERC compliance, Texas RE did not consider ExxonMobil's compliance program as a mitigating factor in determining the penalty.
$18,000 (For TRE201000272, TRE201000273 and TRE201000274)	Self-Report	Luminant submitted a Mitigation Plan on September 3, 2010 to Texas RE outlining its mitigating actions, which included: 1. Verify the completeness of the Registered Entities' Protection System device listing by utilizing protection system electrical drawings and/or physical site inspections; 2. Test the identified relays and current transformers; 3. Place identification labels on the affected relay devices to clearly identify ownership and responsibility for maintenance and testing; 4. Review and update Protection System Maintenance and Testing procedures and processes; 5. Review and modify the Luminant Compliance and Tracking System (LCATS) protective system maintenance and testing activities to ensure timely notifications are distributed to appropriate responsible company personnel. This will provide automatic notifications to ensure maintenance and testing activities are performed in order to meet the required periodicity, and provide management review of testing activities and documentation; and 6. Train appropriate company personnel on updated procedures and processes.	11/16/2011	12/21/2011	Admits	Texas RE considered the compliance program to be a mitigating factor in penalty determination. Luminant is a subsidiary of Energy Future Holdings Corp. (EFH). EFH has a designated corporate compliance office with responsibility to develop, implement, enforce, and maintain the EFH Compliance Program. The compliance office is accountable to the Audit Committee of the EFH Board of Directors and reports to the Audit Committee regarding the administration of the Compliance Program and any proposed substantive changes to the Compliance Program. The Compliance Leadership Team is made up of the heads of Internal Audit, Corporate Security, Human Resources, Compliance, Employment Law and Legal, or their designee(s), and meet as frequently as necessary to coordinate respective activities under the Compliance Program.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$18,000 (For TRE201000272, TRE201000273 and TRE201000274)	Self-Report	Big Brown submitted a Mitigation Plan on September 3, 2010 to Texas RE outlining its mitigating actions, which included: 1. Verify the completeness of the Registered Entities' Protection System device listing by utilizing protection system electrical drawings and/or physical site inspections; 2. Test the identified relays and current transformers; 3. Place identification labels on the affected relay devices to clearly identify ownership and responsibility for maintenance and testing; 4. Review and update Protection System Maintenance and Testing procedures and processes; 5. Review and modify the Luminant Compliance and Tracking System (LCATS) protective system maintenance and testing activities to ensure timely notifications are distributed to appropriate responsible company personnel. This will provide automatic notifications to ensure maintenance and testing activities are performed in order to meet the required periodicity, and provide management review of testing activities and documentation; and 6. Train appropriate company personnel on updated procedures and processes.	11/16/2011	12/21/2011	Admits	Texas RE considered the compliance program to be a mitigating factor in penalty determination. Big Brown is a subsidiary of Luminant Holding Company LLC (LHC), a subsidiary of Energy Future Holdings Corp. Energy Future Holdings Corp. (EFH). EFH has a designated corporate compliance office with responsibility to develop, implement, enforce, and maintain the EFH Compliance Program. The compliance office is accountable to the Audit Committee of the EFH Board of Directors and reports to the Audit Committee regarding the administration of the Compliance Program and any proposed substantive changes to the Compliance Program. The Compliance Leadership Team is made up of the heads of Internal Audit, Corporate Security, Human Resources, Compliance, Employment Law and Legal, or their designee(s), and meet as frequently as necessary to coordinate respective activities under the Compliance Program.
$18,000 (For TRE201000272, TRE201000273 and TRE201000274)	Self-Report	TPC submitted a Mitigation Plan on September 3, 2010 to Texas RE outlining its mitigating actions, which included: 1. Verify the completeness of the Registered Entities' Protection System device listing by utilizing protection system electrical drawings and/or physical site inspections; 2. Test the identified relays and current transformers; 3. Place identification labels on the affected relay devices to clearly identify ownership and responsibility for maintenance and testing; 4. Review and update Protection System Maintenance and Testing procedures and processes; 5. Review and modify the Luminant Compliance and Tracking System (LCATS) protective system maintenance and testing activities to ensure timely notifications are distributed to appropriate responsible company personnel. This will provide automatic notifications to ensure maintenance and testing activities are performed in order to meet the required periodicity, and provide management review of testing activities and documentation; and 6. Train appropriate company personnel on updated procedures and processes.	11/16/2011	12/21/2011	Admits	Texas RE considered the compliance program to be a mitigating factor in penalty determination. TPC is a subsidiary of Luminant Holding Company LLC (LHC), a subsidiary of Energy Future Holdings Corp. Energy Future Holdings Corp. (EFH). EFH has a designated corporate compliance office with responsibility to develop, implement, enforce, and maintain the EFH Compliance Program. The compliance office is accountable to the Audit Committee of the EFH Board of Directors and reports to the Audit Committee regarding the administration of the Compliance Program and any proposed substantive changes to the Compliance Program. The Compliance Leadership Team is made up of the heads of Internal Audit, Corporate Security, Human Resources, Compliance, Employment Law and Legal, or their designee(s), and meet as frequently as necessary to coordinate respective activities under the Compliance Program.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$8,700	Self-Report	On March 4, 2011, ALGS submitted a Mitigation Plan and completed the following activities: (1) Assigned a Team Leader to oversee PRC-005-1 compliance and ensure maintenance and testing of its Protection System devices was appropriately documented; (2) Revised its Maintenance and Testing Procedures to include review and approval by the station manager; (3) Revised its Maintenance and Testing document forms; (4) Implemented the revised Maintenance and Testing procedures; and (5) Added an updated Preventative Maintenance work notification in the Systems Applications and Products (SAP) program.	3/31/2011	11/28/2011	Agrees and Stipulates to the Facts	WECC considered the following mitigating factors in determining the penalty amount: (1) ALGS took voluntary corrective actions to remediate this violation; (2) ALGS self-reported the violation; (3) ALGS's Internal Compliance Program was documented and disseminated throughout the operations staff; ALGS has ICP oversight staff, which is a supervised at a high level in the organization; ALGS has allocated sufficient resources to its ICP and the ICP has the support and participation of the senior management; ALGS reviews and modifies its ICP regularly and the ICP includes formal, internal self-auditing for compliance with the Reliability Standards on a periodic basis; the ICP includes disciplinary action for employees involved in violations of the Reliability Standards; (4) This is not a repeat violation; (5) ALGS was cooperative throughout the compliance process and completed all of WECC's compliance directives; and (6) WECC found no evidence that ALGS attempted to conceal the violation or that the violation was intentional. WECC determined that there were no aggravating factors in determining the penalty amount.
$500	Self-Report	On July 1, 2011, GLEN submitted to WECC a Mitigation Plan (MIT-11-3882) to address the violation of IRO-STD-006-0, WR1. In accordance with the Mitigation Plan, GLEN has taken the following action: (1) reviewed the WebSAS utility training materials used by APM and received written confirmation from APM that all traders have received supplemental training; (2) GLEN's Energy Management group ran a monthly report using WebSAS to verify compliance with the USF standard from January 2010 to June 2011; (3) APM has taken steps to ensure that the audible and visual alarms associated with the WebSAS utility are checked by the trader each day and each shift to ensure they are in working order; and (4) GLEN's Internal Audit Department performed a review of APM's desk procedures and activities, including a spot check of selected transactions.	7/27/2011	8/2/2011	Does Not Contest	WECC determined there were no aggravating factors in determining the penalty amount. GLEN has no prior violations of any Reliability Standards.
$1,000	Self-Report	GRGO immediately restored the PSS to its normal ON operation position after discovering its status on October 12, 2010. According to its Mitigation Plan (MIT-10-3874), GRGO: 1) Conducted refresher training with all operations and management personnel on the PSS and VAR-STD-002b-1; 2) Committed to work with the steam turbine controls vendor to change PSS operational logic, if possible, so that the system defaults to "ON" position following a loss of power; 3) Updated the plant's distributed controls system to include alarm indication when PSS not in service; 4) Updated operator shift rounds to include a check of PSS operation.	1/28/2011	11/18/2011	Does Not Contest	WECC considered the following factors in determining the penalty amount: GRGO's violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, the violation was self-reported, there were no aggravating factors in determining the penalty amount, and the violation did not pose an ongoing risk to the BPS.

Total Penalty or Sanction ($)	Method of Discovery	Description of Mitigation Activity	Mitigation Completion Date	Date Regional Entity Verified Completion of Mitigation	"Admits" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$1,000 (Settlement of WECC201102909, WECC201102910, WECC201102911, WECC201102912)	Self-Report	NCPA submitted a Mitigation Plan which outlined the following mitigation activities: 1) Work with area coordinator PGAE to determine all data requirements; 2) Develop a procedure and process to ensure that all required data is checked and sent to the area coordinator, and reviewed for accuracy prior to submitting data to WECC; and 3) Assign individuals or third party responsibility for following the procedure and process for data submittal to the area coordinator. The mitigation relates to both submittals to PGAE and from PGAE before it goes to WECC.	11/23/2011	12/21/2011	Does not contest	NCPA does not have a formal ICP documented with WECC, however it has a good compliance program with respect to its violation history. NCPA took voluntary corrective action to remediate these violations, NCPA self-reported these violations, NCPA was cooperative throughout the process, NCPA did not fail to complete any applicable compliance directives, and there was no evidence of any attempt by NCPA to conceal these violations. Further, NCPA did not have any aggravating factors. WECC did not give NCPA mitigating credit for the ICP.
$1,000 (Settlement of WECC201102909, WECC201102910, WECC201102911, WECC201102912)	Self-Report	NCPA submitted a Mitigation Plan which outlined the following mitigation activities: 1) Work with area coordinator PGAE to determine all data requirements; 2) Develop a procedure and process to ensure that all required data is checked and sent to the area coordinator, and reviewed for accuracy prior to submitting data to WECC; and 3) Assign individuals or third party responsibility for following the procedure and process for data submittal to the area coordinator. The mitigation relates to both submittals to PGAE and from PGAE before it goes to WECC.	11/23/2011	12/21/2011	Does not contest	NCPA does not have a formal ICP documented with WECC, however it has a good compliance program with respect to its violation history. NCPA took voluntary corrective action to remediate these violations, NCPA self-reported these violations, NCPA was cooperative throughout the process, NCPA did not fail to complete any applicable compliance directives, and there was no evidence of any attempt by NCPA to conceal these violations. Further, NCPA did not have any aggravating factors. WECC did not give NCPA mitigating credit for the ICP.
$1,000 (Settlement of WECC201102909, WECC201102910, WECC201102911, WECC201102912)	Self-Report	NCPA submitted a Mitigation Plan which outlined the following mitigation activities: 1) Work with area coordinator PGAE to determine all data requirements; 2) Develop a procedure and process to ensure that all required data is checked and sent to the area coordinator, and reviewed for accuracy prior to submitting data to WECC; and 3) Assign individuals or third party responsibility for following the procedure and process for data submittal to the area coordinator. The mitigation relates to both submittals to PGAE and from PGAE before it goes to WECC.	11/23/2011	12/21/2011	Does not contest	NCPA does not have a formal ICP documented with WECC, however it has a good compliance program with respect to its violation history. NCPA took voluntary corrective action to remediate these violations, NCPA self-reported these violations, NCPA was cooperative throughout the process, NCPA did not fail to complete any applicable compliance directives, and there was no evidence of any attempt by NCPA to conceal these violations. Further, NCPA did not have any aggravating factors. WECC did not give NCPA mitigating credit for the ICP.

Attachment A-1

December 30, 2011 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" "Neither Admits nor Denies" "Agrees and Stipulates to the Facts" or "Does Not Contest"	Other Factors Affecting the Penalty Determination, including Compliance History, Internal Compliance Program and Compliance Culture
$1,000 (Settlement of WECC201102909, WECC201102910, WECC201102911, WECC201102912)	Self-Report	NCPA submitted a Mitigation Plan which outlined the following mitigation activities: 1) Work with area coordinator PGAE to determine all data requirements; 2) Develop a procedure and process to ensure that all required data is checked and sent to the area coordinator, and reviewed for accuracy prior to submitting data to WECC; and 3) Assign individuals or third party responsibility for following the procedure and process for data submittal to the area coordinator. The mitigation relates to both submittals to PGAE and from PGAE before it goes to WECC.	11/23/2011	12/21/2011	Does not contest	NCPA does not have a formal ICP documented with WECC, however it has a good compliance program with respect to its violation history. NCPA took voluntary corrective action to remediate these violations, NCPA self-reported these violations, NCPA was cooperative throughout the process, NCPA did not fail to complete any applicable compliance directives, and there was no evidence of any attempt by NCPA to conceal these violations. Further, NCPA did not have any aggravating factors. WECC did not give NCPA mitigating credit for the ICP.

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100223	Settlement Agreement	NPCC_URE1 Self Reported a violation of CIP-004-1 R4 to NPCC. NPCC determined that NPCC_URE1 was in violation of the Standard. NPCC_URE1 failed to review the list of its personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets quarterly, as required by the Standard. Specifically, NPCC_URE1 did not review the list of personnel who were in possession of keys that allowed Physical Security Perimeter (PSP) substation access in the cases where the card reader was out of service. Additionally, NPCC_URE1 failed to revoke access within the proper timeframe (seven days) for personnel who no longer needed to be in possession of those keys. Approximately 30-50 keys were unaccounted for from when NPCC_URE1 was required to comply with the Standard to when new locks and keys were installed.	CIP-004-1	R4	Medium	Severe	NPCC determined that this violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE1 has processes in place to ensure that only authorized personnel are allowed access to the substation. Specifically, there is and was at the time of the violation a documented key system in place to track key access to the outer gate. There is also a background check required for gate access. Additionally, the standard method of accessing the substation is a swipe card, and there was and is a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning; at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable and are useless with gate access. Second, NPCC_URE1 has alarms generated immediately to Security if the card reader is bypassed using the key. Third, there was no actual impact as there were no incidents at NPCC_URE1 facilities related to the lack of proper documentation and revocation of the keys.	When the Standard became mandatory and enforceable	When the new lock system was implemented
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 1 (NPCC_URE1)	NCRXXXXX	NPCC201100224	Settlement Agreement	NPCC_URE1 Self Reported a violation of CIP-006-1 R1 to NPCC. NPCC determined that NPCC_URE1 was in violation of the Standard. NPCC_URE1 failed to create and maintain a physical security plan to address procedures for the appropriate use of physical access controls, as required by the Standard. Specifically, NPCC_URE1 did not have a procedure in place to document: (1) the appropriate use of keys that granted PSP substation access; or (2) the appropriate response to loss of such keys that allowed entrance into the PSP. Approximately 30-50 keys were unaccounted for from when NPCC_URE1 was required to comply with the Standard to when new locks and keys were installed.	CIP-006-1	R1	Medium	Severe	NPCC determined that this violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE1 has processes in place to ensure that only authorized personnel are allowed access to the substation. Specifically, there is and was at the time of the violation a documented key system in place to track key access to the outer gate. There is also a background check required for gate access. Additionally, the standard method of accessing the substation is a swipe card, and there was and is a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning; at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable and are useless with gate access. Second, NPCC_URE1 has alarms generated immediately to Security if the card reader is bypassed using the key. Third, there was no actual impact as there were no incidents at NPCC_URE1 facilities due to inappropriate use of keys.	When the Standard became mandatory and enforceable	When the new lock system was implemented

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC201100225	Settlement Agreement	NPCC_URE2 self-reported a violation of CIP-004-1 R4 to NPCC. NPCC determined that URE was in violation of the Standard. NPCC_URE2 failed to review the list of its personnel who have authorized cyber or authorized unescorted physical access to Critical Cyber Assets quarterly, as required by the Standard. Specifically, NPCC_URE2 did not review the list of personnel who were in possession of keys that allowed Physical Security Perimeter (PSP) substation access in the cases where the card reader was out of service. Additionally, NPCC_URE2URE failed to revoke access within the proper timeframe (seven days) for personnel who no longer needed to be in possession of those keys. Approximately 30-50 keys were unaccounted for from when NPCC_URE2 was required to comply with the Standard to when new locks and keys were installed.	CIP-004-1	R4	Medium	Severe	NPCC determined that this violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 has processes in place to ensure that only authorized personnel are allowed access to the substation. Specifically, there is and was at the time of the violation a documented key system in place to track key access to the outer gate. There is also a background check required for gate access. Additionally, the standard method of accessing the substation is a swipe card, and there was and is a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning; at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable and are useless with gate access. Second, NPCC_URE2 has alarms generated immediately to Security if the card reader is bypassed using the key. Third, there was no actual impact as there were no incidents at NPCC_URE2 facilities related to the lack of proper documentation and revocation of the keys.	When the Standard became mandatory and enforceable	When the new lock system was implemented
Northeast Power Coordinating Council, Inc. (NPCC)	Unidentified Registered Entity 2 (NPCC_URE2)	NCRXXXXX	NPCC201100226	Settlement Agreement	NPCC_URE2 self-reported a violation of CIP-006-1 R1 to NPCC. NPCC determined that NPCC_URE2 was in violation of the Standard. NPCC_URE2 failed to create and maintain a physical security plan to address procedures for the appropriate use of physical access controls, as required by the Standard. Specifically, NPCC_URE2 did not have a procedure in place to document: (1) the appropriate use of keys that granted PSP substation access; or (2) the appropriate response to loss of such keys that allowed entrance into the PSP. Approximately 30-50 keys were unaccounted for from NPCC_URE2 was required to comply with the Standard to when new locks and keys were installed.	CIP-006-1	R1	Medium	Severe	NPCC determined that this violation posed a minimal risk and not serious or substantial risk to the reliability of the bulk power system (BPS) because NPCC_URE2 has processes in place to ensure that only authorized personnel are allowed access to the substation. Specifically, there is and was at the time of the violation a documented key system in place to track key access to the outer gate. There is also a background check required for gate access. Additionally, the standard method of accessing the substation is a swipe card, and there was and is a procedure in place for tracking and revoking swipe card access. The keys at issue here are used only in the event that the swipe card system is not functioning; at no time during the violation did the swipe card system fail to force the use of the keys. These keys are numbered but otherwise unidentifiable and are useless with gate access. Second, NPCC_URE2 has alarms generated	When the Standard became mandatory and enforceable	When the new lock system was implemented

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
ReliabilityFirst Corporation (ReliabilityFirst)	Unidentified Registered Entity 1, Unidentified Registered Entity 2, Unidentified Registered Entity 3, Unidentified Registered Entity 4 (collectively, RFC_URE1) **GenOn REMA 1, GenOn REMA 2, GenOn REMA 3, and GenOn REMA 4 (collectively, the GenOn Entities), successors in interest to RRI Energy Mid-Atlantic Holdings, LLC (REMA)**	NCRXXXXX, NCRXXXXX, NCRXXXXX, NCRXXXXX	RFC201000391	Settlement Agreement	RFC_URE1 self-reported a violation of CIP-006-2 R1.6 to ReliabilityFirst. The retail business of RFC_URE1's parent company was sold. During a subsequent period, including the time period relevant to this violation, the parent company and purchasing company shared certain spaces. Specifically, the purchasing company's data storage servers were located in the same locked room as RFC_URE1's data storage servers. RFC_URE1's data storage servers were located in locked cabinets within this room. These servers were capable of performing as RFC_URE1's backup control center, and as such, RFC_URE1 considered them as Critical Cyber Assets (CCAs). According to the Self-Report, an employee of the purchasing company escorted a visitor inside the Physical Security Perimeter (PSP) surrounding these servers. This individual failed to document the entry of the visitor into the PSP. After entering the PSP, the visitor was left unescorted for 25 minutes. The visitor was a computer manufacturer vendor. RFC_URE1 discovered the violation while checking the access logs for the PSP. Upon discovery of the possible violation, RFC_URE1 ensured the access rights of the purchasing company's employee who left the computer manufacturer vendor unescorted within the PSP were terminated.	CIP-006-2	R1/1.6	Medium	Severe	This violation posed a moderate risk to the bulk power system (BPS) because failure to continuously escort personnel who do not have authorized physical access to a PSP poses an increased risk to CCAs essential to the operation of the BPS. This violation did not pose a serious or substantial risk to the reliability of the BPS because, while a visitor did enter RFC_URE1's PSP and remained within that perimeter unescorted for 25 minutes, RFC_URE1's CCAs were located in fully enclosed and locked cabinets, which the unescorted visitor could not and did not access. Furthermore, the data center was under video surveillance, which confirmed that the unescorted visitor did not approach RFC_URE1's assets.	The date RFC_URE1 failed to ensure an unauthorized visitor to its PSP was continuously escorted while inside the PSP	The date RFC_URE1 failed to ensure an unauthorized visitor to its PSP was continuously escorted while inside the PSP
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000288	Settlement Agreement	During a Spot Check, the SPP RE found that SPP RE_URE1's Cyber Security Policy (Policy) did not address all of the requirements of CIP-002-1 through CIP-009-1 as required by CIP-003-1 R1.1. For example, its Policy did not address the requirement for authentication of access into the electronic security perimeter required by CIP-005-1 R2.5. Also, the Policy had no reference to the vulnerability assessment required by CIP-005-1 R4. Also, SPP RE_URE1 had not updated its Policy to reflect Version 2 of the CIP Standards that were in effect at the time of the Spot Check. For example, the Policy provided for a 90-day period to update the Incident Response Reporting Procedure following any changes, which was consistent with CIP-008-1 R1.4, while CIP-008-2 R1.4 required a process to ensure that updates occur within a shorter 30-day period.	CIP-003-1	R1.1	Lower	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-003-1 R1.1 posed a minimal risk to the reliability of the bulk power system (BPS) and did not pose a serious or substantial risk because the deficiency was documentation-related, involving the SPP RE_URE1 Policy itself. SPP RE_URE1 had a Policy in place that addressed most, though not all, of the CIP-002 through CIP-009 requirements.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000289	Settlement Agreement	During a Spot Check, the SPP RE found SPP RE_URE1 could not provide evidence of the testing of cyber security controls for a Microsoft security patch implementation on the SPP RE_URE1 system, in violation of this Standard. SPP RE_URE1 submitted additional evidence to rebut the Spot Check team's finding, stating that at the Spot Check SPP RE_URE1's Subject Matter Expert (SME) incorrectly provided that the patch was implemented and that the test records were actually collected when the Microsoft patch was implemented the next month. The SPP RE determined that the evidence submitted by SPP RE_URE1 was still insufficient because the test records did not show that SPP RE_URE1 had tested its cyber security controls to verify that the Microsoft security patch did not adversely impact the security of its affected Cyber Assets.	CIP-007-1	1.3	Lower	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R1.3 posed a moderate risk to the reliability of the bulk power system (BPS) and did not pose a serious or substantial risk because SPP RE_URE1 was applying security patches on its system although it failed to test the security controls prior to implementation of a Microsoft security patch.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000394	Settlement Agreement	SPP RE_URE1 reported in its Self-Certification that it was not in compliance with CIP-005-2 R1.5 because of its potential violations of CIP-003-1 R4 and R6, CIP-005-1 R2 and R3, and CIP-007-1 R3, R5, R6, R8, and R9. SPP RE_URE1 was not fully compliant with a number of the requirements related to the protection of its Critical Cyber Assets (CCAs), but also regarding protection of its Cyber Assets used for Electronic Security Perimeter (ESP) access control and/or monitoring.	CIP-005-1	1.5	Medium	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-005-1 R1.5 posed a moderate risk to the reliability of the bulk power system (BPS) but did not pose a serious or substantial risk. SPP RE_URE1's failure to afford several of the required protective measures to its CAs used in ESP access control and/or monitoring and its failure to provide protection to its CCAs within its ESP rendered its system more vulnerable to attack.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000395	Settlement Agreement	SPP RE_URE1 reported in its Self-Certification that it was not in compliance with CIP-005-2 R2 because it had not documented configurations for all ports and services on Critical Cyber Assets (CCAs). Additionally, SPP RE_URE1 did not have explicit default deny rules set for outbound communications through one firewall that was protecting a web console server, and it did not have technical procedures to log unauthorized outbound communications from both trusted and entrusted interfaces.	CIP-005-1	2	Medium	High	The SPP RE determined that SPP RE_URE1's violation of CIP-005-1 R2 posed a minimal risk to the reliability of the bulk power system (BPS) and did not pose a serious or substantial risk because SPP RE_URE1 followed the required manufacturer (Siemens) configurations for ports and services which represent the majority of its Critical Cyber Asset (CCA) equipment. SPP RE_URE1 had also implemented a control mode that denies by default on most of its electronic access points to the SPP RE_URE1 ESP. The only electronic access point without deny by default settings was at the web console server, which was used solely for capturing and transmitting EMS/SCADA images. Only outbound communications, not inbound communications, were missing deny by default protection.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000396	Settlement Agreement	SPP RE_URE1 reported in its Self-Certification that it was not compliant with CIP-005-2 R3 because SPP RE_URE1 had not developed a logging and monitoring program for unauthorized attempts and access within its Energy Management System (EMS) network for all access points of its Electronic Security Perimeter (ESP). Additionally, SPP RE_URE1 did not have a logging procedure for security events for Linux OS, Windows, firewalls, switches and routers.	CIP-005-1	3	Medium	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-005-1 R3 posed a moderate risk to the reliability of the bulk power system (BPS) and did not pose a serious or substantial risk because, SPP RE_URE1 began to use TripWire to monitor its system. However, SPP RE_URE1 was not utilizing a logging and monitoring process prior to TripWire and the TripWire program did not monitor all EMS access points on the SPP RE_URE1 ESP. Due to the lack of a monitoring and logging program to monitor electronic access for all EMS access points within its ESP, SPP RE_URE1 did not have a method of detecting whether or not unauthorized attempts or access had occurred on its system. This left the ESP vulnerable to attacks and made it difficult to monitor for suspicious activity that may have occurred on the SPP RE_URE1 system, therefore decreasing the likelihood of early detection of a cyber attack and creating a moderate risk to the BPS.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000397	Settlement Agreement	SPP RE_URE1 reported in its Self-Certification that it was not compliant with CIP-005-2 R4 because SPP RE_URE1 had not developed a procedure to describe its vulnerability assessment process. Specifically, SPP RE_URE1 had not identified the steps utilized in performing the vulnerability assessment, the process for identifying the results of the vulnerability assessment, and it had not created an action plan to remediate or mitigate any vulnerabilities identified in the assessment. Additionally, SPP RE_URE1 could not provide evidence that it reviewed default accounts, passwords and Simple Network Management Protocol (SNMP) community strings inside its Electronic Security Perimeter (ESP) as part of its vulnerability assessment. SPP RE_URE1 performed its first vulnerability assessment on its ESP about ten months past the date it was required to comply with CIP-005-1 R4.	CIP-005-1	4	Medium	Severe	The SPP RE determined that SPP RE_URE1's violation of CIP-005-1 R4 posed a moderate risk to the reliability of the bulk power system (BPS) but did not pose a serious or substantial risk because although SPP RE_URE1 had an outside contractor perform a vulnerability assessment, it did not utilize the results of the vulnerability assessment to create and implement action plans to remediate or mitigate the vulnerabilities that were identified. Because SPP RE_URE1 did not implement action plans to mitigate the vulnerabilities regarding the electronic access points on its ESP, there was not a guarantee that its ESP was secure. Further, because SPP RE_URE1 had not formally documented its vulnerability assessment process, there was a risk that the assessment would not be performed thoroughly and consistently. The vulnerability assessment conducted was in fact missing some elements required by CIP-005 R4.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000399	Settlement Agreement	SPP RE_URE1 reported in its Self Certification, that it was not compliant with CIP-007-2 R2 because SPP RE_URE1 had not documented the proper configurations of enabled ports and services for all of its network devices within the Electronic Security Perimeter (ESP). Because there was not a documented baseline for comparison, SPP RE_URE1 was unable to determine if solely the ports and services required for normal and emergency operations of some of its devices were enabled at any given time. However, for all of its Siemens devices, SPP RE_URE1 had enabled and documented the ports and services that were required for operations. SPP RE_URE1 relied on the Security Administration Manual (Manual) supplied by Siemens to identify the ports and services that are required for its Energy Management System (EMS). Section 6.4 of the Manual lists the various unnecessary ports that should be disabled and the procedure for doing so. In Section 11.0, the Manual also provides details regarding which ports should be enabled to provide proper functioning to the SPP RE_URE1 EMS. SPP RE_URE1 verified that these are the only enabled ports during the installation of new Versions of software and also performed a review of the services file on each machine during the annual assessment of its Critical Cyber Assets (CCAs) inside the ESP.	CIP-007-1	2	Medium	Moderate	The SPP RE has determined that SPP RE_URE1's violation of CIP-007-1 R2 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because SPP RE_URE1 had documented its ports and services for all of its Siemens devices within the ESP, and these devices were monitored by the SPP RE_URE1 EMS SCADA system. The Siemens devices within the ESP are deemed to be the most critical devices within the ESP. For all of its Siemens devices, SPP RE_URE1 had enabled and documented the ports and services that were required for operations and verified that these are the only enabled ports during the installation of new versions of software. SPP RE_URE1 also performed a review of the services file on each machine during the annual assessment of its Critical Cyber Assets (CCAs) inside the ESP.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000400	Settlement Agreement	SPP RE_URE1 reported in its Self-Certification that it was not compliant with CIP-007-2 R3. SPP RE determined that SPP RE_URE1 did not document the reasons why certain security patches were not selected to be installed on Cyber Assets (CAs) within the Electronic Security Perimeter (ESP). SPP RE_URE1 did not document the compensating measures applied to mitigate risk exposure or an acceptance of risk when a security patch was not chosen for installation. However, SPP RE_URE1 had evaluated all security patches that were installed within its ESP and documented when a security patch was installed.	CIP-007-1	3	Lower	Severe	The SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R3 posed a minimal risk and did not pose a serious or substantial risk to reliability of the bulk power system (BPS) because SPP RE_URE1 had documented when security patches were installed for CAs within the ESP and the reason why a particular security patch was installed. Because SPP RE_URE1 was reviewing all security patches to determine whether or not a patch should be installed, the violation had a minimal impact on the reliability of the BPS because SPP RE_URE1 was only lacking the documentation of the rationale for not installing particular security patches.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000401	Settlement Agreement	SPP RE_URE1 reported in its Self Certification that it was not compliant with CIP-007-2 R5 because it had not established, implemented, and documented sufficient controls to enforce the access authentication of, and accountability for, all user activity on individual and shared user accounts. SPP RE_URE1 did not have a policy in place to ensure that user accounts were implemented and approved by designated personnel, as required by R5.1.1. Further, SPP RE_URE1's system logs were not capturing data on its network devices sufficient to maintain 90-day audit trails of user account activity as required by R5.1.2. SPP RE_URE1 did not perform an annual review of specific access privileges to its Critical Cyber Assets (CCAs) for 2009. With regard to R5.2, SPP RE_URE1 did not have a policy for managing its shared and generic account privileges and did not maintain a list of persons with access to those accounts.	CIP-007-1	5	Lower	Severe	The SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R5 posed a moderate risk but did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because although SPP RE_URE1 was not managing a proper environment for security, it had been performing an annual review of the general access privileges to its CCAs. Because SPP RE_URE1 was not reviewing specific access privileges to its CCAs, the potential existed for someone to falsify an account and have free use of SPP RE_URE1's system. In failing to adequately monitor its system, SPP RE_URE1 left its system more vulnerable to attack, which in turn created reliability risk to its system and the BPS.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000402	Settlement Agreement	SPP RE_URE1 reported in its Self Certification that it was not compliant with CIP-007-2 R6 because SPP RE_URE1 had not implemented tools or controls to monitor for, alert personnel of, and retain and review logs of security events on Cyber Assets (CAs) within the Electronic Security Perimeter (ESP) on the Energy Management System (EMS) network and SPP RE_URE1 failed to create a program to log, monitor, identify, review and react to security events on all Cyber Assets within the ESP.	CIP-007-1	6	Lower	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R6 posed a moderate and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because SPP RE_URE1 began to use TripWire to monitor its system. However, prior to that date, the entity did not have an alternative system in place to monitor its system and TripWire program did not monitor all CAs within the EMS network. Due to the lack of a monitoring and logging program to monitor CAs within the EMS network, SPP RE_URE1 did not have a method of detecting whether or not unauthorized attempts to tamper with the CAs had occurred within the EMS network. This left SPP RE_URE1's CAs vulnerable to attacks and made it difficult to monitor for suspicious activity that may have occurred on the SPP RE_URE1 system, therefore decreasing the likelihood of early detection of a cyber attack and creating a moderate risk to the BPS.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000403	Settlement Agreement	SPP RE_URE1 reported in its Self Certification that it was not compliant with CIP-007-2 R8 because SPP RE_URE1 had not developed a procedure describing its vulnerability assessment process. SPP RE_URE1 had not identified the steps that it utilized to perform the vulnerability assessment and to review and document the results. Further, SPP RE_URE1 had not created an action plan to remediate or mitigate any vulnerabilities identified in the assessment. Additionally, SPP RE_URE1 could not provide evidence that it reviewed controls for default accounts as required by R8.3. SPP RE_URE1 performed its first vulnerability assessment on its Critical Assets (CAs) within its ESP about ten months past the date it was required to comply with CIP-007-1 R8.	CIP-007-1	8	Lower	Severe	SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R8 posed a moderate risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). Although SPP RE_URE1 performed a vulnerability assessment, it did not utilize the results of the vulnerability assessment to create and implement action plans to remediate or mitigate the vulnerabilities that were identified. Because SPP RE_URE1 did not implement action plans to mitigate the vulnerabilities regarding the electronic access points on its ESP, there was not reasonable assurance that its ESP was secure. Vulnerabilities that were identified in the assessment included, but were not limited to, firewall rules that did not ensure access was denied by default, the lack of a centralized logging and monitoring process, and some users on the SPP RE_URE1 system logging into the system under the root password. Further, because SPP RE_URE1 had not formally documented its vulnerability assessment process, there was a risk that the assessment would not be performed thoroughly and consistently. The vulnerability assessment conducted was in fact missing some elements required by CIP-007-1 R8.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed
Southwest Power Pool RE (SPP RE)	Unidentified Registered Entity 1 (SPP RE_URE1)	NCRXXXXX	SPP201000404	Settlement Agreement	SPP RE_URE1 reported in its Self Certification that it was not compliant with CIP-007-2 R9 because SPP RE_URE1 did not have documentation that it had performed an annual review of the documents and procedures it maintains pursuant to CIP-007. Additionally, SPP RE_URE1 failed to document changes resulting from modifications to the systems and controls required under CIP-007 within ninety calendar days of those changes.	CIP-007-1	9	Lower	Severe	The SPP RE determined that SPP RE_URE1's violation of CIP-007-1 R9 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because it had documentation and procedures referenced in CIP-007 but did not have evidence that it reviewed and updated its documentation annually. Therefore, this is an issue of documentation and SPP RE_URE1's lack of performance is addressed in its corresponding CIP-007 violations.	The date SPP RE_URE1 was required to comply with the Reliability Standard	The date the Mitigation Plan was completed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000130	Settlement Agreement	Texas RE_URE1 is required under CIP-005-1 R2, at all access points to the Electronic Security Perimeter (ESP), to enable only ports and services required for operations and to monitor Cyber Assets within the ESP, and to document the configuration of those ports and services. Texas RE_URE1 determined it was necessary to increase the level of detail in its procedures, programs, supporting documentation, and evidence regarding the CIP-002 through CIP-009 Reliability Standards. As a result, all scans and associated enabling/disabling of ports and services which should have been completed by a certain time but were not completed until almost a month later, when Texas RE_URE1's ports and services acceptability procedure document was approved, dated and signed.	CIP-005-1	R2; R2.2	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not verifying and providing documentation and proof of controlling performance between when it was required to comply with the Standard and it when it afforded a possible intruder the opportunity to gain unauthorized access into the ESP. However, Texas RE_URE1 reported that it had in place certain compensating measures to mitigate risk including two firewalls and physical access restrictions. Texas RE_URE1 reported that the appropriate ports and services were enabled and disabled all along but that it had failed to timely document them. Lastly, Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-005-1	Mitigation Plan Completion
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000132	Settlement Agreement	Texas RE_URE1 is required under CIP-005-1 R2, at all access points to the Electronic Security Perimeter (ESP), to enable only ports and services required for operations and to monitor Cyber Assets within the ESP, and to document the configuration of those ports and services. Texas RE_URE1 determined it was necessary to increase the level of detail in its procedures, programs, supporting documentation, and evidence regarding the CIP-002 through CIP-009 Reliability Standards. As a result, all scans and associated enabling/disabling of ports and services which should have been completed by a certain time but were not completed until almost a month later, when Texas RE_URE1's ports and services acceptability procedure document was approved, dated and signed.	CIP-005-1	R2; R2.2	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not verifying and providing documentation and proof of controlling performance between when it was required to comply with the Standard and it when it afforded a possible intruder the opportunity to gain unauthorized access into the ESP. However, Texas RE_URE1 reported that it had in place certain compensating measures to mitigate risk including two firewalls and physical access restrictions. Texas RE_URE1 reported that the appropriate ports and services were enabled and disabled all along but that it had failed to timely document them. Lastly, Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-005-1	Mitigation Plan Completion

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000131	Settlement Agreement	Texas RE_URE1 is required under CIP-005-1 R4, to perform a cyber vulnerability assessment of the electronic access points to the ESP at least annually, which is to include certain information. Texas RE_URE1 determined it was necessary to increase the level of detail in its procedures, programs, supporting documentation, and evidence regarding the CIP-002 through CIP-009 Reliability Standards. As a result, Texas RE_URE1 did not complete the following until early in 2010: a document identifying the vulnerability assessment process; its review to verify that only ports and services required for operations at electronic access points was enabled; its review of controls for default accounts, passwords, and network management community strings; and document the results of the assessment.	CIP-005-1	R4; R4.1; R4.2; R4.4; R4.5	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not verifying and providing documentation and proof of controlling performance between the date it was required to comply with the Standard and when it afforded a possible intruder the opportunity to gain unauthorized access into the ESP. However, Texas RE_URE1 reported that it had in place certain compensating measures to mitigate risk including two firewalls and physical access restrictions. Texas RE_URE1 reported that the appropriate ports and services were enabled and disabled all along but that it had failed to timely document them. Lastly, Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-005-1	The date on which Texas RE_URE1 completed documenting its cyber vulnerability assessment process
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE202000133	Settlement Agreement	Texas RE_URE1 is required under CIP-005-1 R4, to perform a cyber vulnerability assessment of the electronic access points to the ESP at least annually, which is to include certain information. Texas RE_URE1 determined it was necessary to increase the level of detail in its procedures, programs, supporting documentation, and evidence regarding the CIP-002 through CIP-009 Reliability Standards. As a result, Texas RE_URE1 did not complete the following until early in 2010: a document identifying the vulnerability assessment process; its review to verify that only ports and services required for operations at electronic access points; its review of controls for default accounts, passwords, and network management community strings; and document the results of the assessment.	CIP-005-1	R4; R4.1; R4.2; R4.4; R4.5	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not verifying and providing documentation and proof of controlling performance between the date it was required to comply with the Standard and when it afforded a possible intruder the opportunity to gain unauthorized access into the ESP. However, Texas RE_URE1 reported that it had in place certain compensating measures to mitigate risk including two firewalls and physical access restrictions. Texas RE_URE1 reported that the appropriate ports and services were enabled and disabled all along but that it had failed to timely document them. Lastly, Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-005-1	The date on which Texas RE_URE1 completed documenting its cyber vulnerability assessment process

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000227	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R2, to enable only those ports and services required for normal and emergency operations. Texas RE_URE1 did this for 84.6% of its servers by the date it was required to be compliant the rest were enabled prior to the end of the month. The Standard further requires that Texas RE_URE1 disable all other ports and services prior to production use of all Cyber Assets inside the ESP. Texas RE_URE1 did this for 80.8% of its servers by the date it was required to be compliant the rest were disabled prior to the end of the month. Where unused ports and services cannot be disabled due to technical limitations, Texas RE_URE1 is required under the Standard to document compensating measures applied to mitigate risk exposure or an acceptance of risk. Texas RE_URE1 completed this documentation for 80.8% of its servers by the date it was required to be compliant the rest were documented prior to the end of the month. Thus in each instance, Texas RE_URE1 was in violation of the Standard for less than a month.	CIP-007-1	R2; R2.1; R2.2; R2.3	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled for the duration of this violation. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	The last date Texas RE_URE1 was out of compliance with CIP-007-1 R2
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000233	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R2, to enable only those ports and services required for normal and emergency operations. Texas RE_URE1 did this for 84.6% of the servers by the date it was required to be compliant and the rest were enabled by the end of the month. The Standard further requires that Texas RE_URE1 disable all other ports and services prior to production use of all Cyber Assets inside the ESP. Texas RE_URE1 did this for 80.8% of its servers by the date it was required to be compliant the rest were disabled by the end of the month. Where unused ports and services cannot be disabled due to technical limitations, Texas RE_URE1 is required under the Standard to document compensating measures applied to mitigate risk exposure or an acceptance of risk. Texas RE_URE1 completed this documentation for 80.8% of its servers by the date it was required to be compliant the rest were documented prior to the end of the month. Thus in each instance, Texas RE_URE1 was in violation of the Standard for less than a month.	CIP-007-1	R2; R2.1; R2.2; R2.3	Medium	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled for the duration of this violation. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	The last date Texas RE_URE1 was out of compliance with CIP-007-1 R2

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000230	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R6, to ensure that its Cyber Assets within the ESP have security monitoring tools which issue automated or manual alerts for detected Cyber Security Incidents. Between the date it was required to be compliant and the first two weeks, 15.8% of Texas RE_URE1's Cyber Assets were not monitored preventing recognition of automated or manual alerts issued for detected Cyber Security Incidents.	CIP-007-1	R6; R6.2	Lower	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled for the duration of this violation. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	When proper monitoring resumed
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000236	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R6, to ensure that its Cyber Assets within the ESP have security monitoring tools which issue automated or manual alerts for detected Cyber Security Incidents. Between the date it was required to be compliant and the first two weeks 5.8% of Texas RE_URE1's Cyber Assets were not monitored preventing recognition of automated or manual alerts issued for detected Cyber Security Incidents.	CIP-007-1	R6; R6.2	Lower	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled all along. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	When proper monitoring resumed

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000232	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R8, to perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually. Texas RE_URE1 failed to comply with this Standard in several respects. First, Texas RE_URE1 did not complete and approve its Cyber Asset Vulnerability Assessment Process document until almost a month after it was required to comply with the Standard. Second, for 15.4% of its servers, Texas RE_URE1 did not finalize all work necessary to verify that only those ports and services required for normal and emergency operations were enabled until almost a month after it was required to comply with the Standard. Third, Texas RE_URE1 finalized its review of controls for default accounts and finalized the results of the assessment almost a month after it was required to comply with the Standard.	CIP-007-1	R8; R8.1; R8.2; R8.3; R8.4	Lower	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled all along. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	The date Texas RE_URE1 had a vulnerability assessment process document
Texas Reliability Entity, Inc. (Texas RE)	Unidentified Registered Entity 1 (Texas RE_URE1)	NCRXXXXX	TRE201000238	Settlement Agreement	Texas RE_URE1 is required under CIP-007-1 R8, to perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually. Texas RE_URE1 failed to comply with this Standard in several respects. First, Texas RE_URE1 did not complete and approve its Cyber Asset Vulnerability Assessment Process document until almost a month after it was required to comply with the Standard. Second, for 15.4% of its servers, Texas RE_URE1 did not finalize all work necessary to verify that only those ports and services required for normal and emergency operations were enabled until almost a month after it was required to comply with the Standard. Third, Texas RE_URE1 finalized its review of controls for default accounts and finalized the results of the assessment almost a month after it was required to comply with the Standard.	CIP-007-1	R8; R8.1; R8.2; R8.3; R8.4	Lower	N/A (VSLs for NERC Standards CIP-002 through CIP-009 were not approved by FERC until March 18, 2010).	Texas RE determined that this violation posed a moderate but not serious or substantial risk to the reliability of the bulk power system (BPS). Texas RE_URE1, by not documenting and/or verifying performance, afforded a possible intruder the opportunity to gain unauthorized access into the ESP. The potential risk to the BPS was moderate as the correct and appropriate ports and services were enabled/disabled all along. The procedures described were of a verification and documentation nature for purposes of complying with CIP-007-1. In addition, the violation period was relatively brief and Texas RE_URE1 indicated that there were no breaches of security for the time period in question.	The date on which Texas RE_URE1 was subject to compliance with CIP-007-1	The date Texas RE_URE1 had a vulnerability assessment process document

Attachment A-2

December 30, 2011 Public Spreadsheet Notice of Penalty Spreadsheet

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

Region	Registered Entity	NCR_ID	NERC Issue Tracking #	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	WECC201102598	Notice of Confirmed Violation	WECC_URE1 submitted a Self-Report stating that it failed to secure Cyber Assets provisioning physical access control and monitoring (PACM) to its Physical Security Perimeters (PSPs) in violation of CIP-006-1 R1 R1.8. WECC determined that the scope of the violation included fourteen Cyber Assets. Specifically, WECC determined that WECC_URE1 failed to identify two Cyber Assets as Cyber Assets provisioning access control and monitoring. Further WECC determined that WECC_URE1 failed to afford protective measures described under CIP-005-1 R2, CIP-007-1 R2, R3, R5 and R8, and CIP-009-1 R5 to three Cyber Assets; and, WECC_URE1 did not afford two protective measures (CIP-008-1 R8 and CIP-009-1 R5) to nine Cyber Assets provisioning access control and monitoring.	CIP-006-1	R1; R1.8	Lower	Severe	WECC determined that the violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS) because the risk was offset given the limited scope of WECC_URE1's violation. Nine of the twelve devices in scope were identified as Cyber Assets provisioning access control and monitoring. Even Cyber Assets that were not identified as access points, were equipped with protections that limited access. WECC_URE1's PACM network design. WECC_URE1's PSPs are dedicated to a specific network, which operates in a complete isolation, thus reducing the risk to the BPS. Further, the PACM network itself is physically and electronically isolated, and access to it is controlled and monitored.	The date on which WECC_URE1 was required to be compliant with CIP-006-1	The date on which WECC_URE1 revised its physical security plan to comply with R1.8

Attachment A-2

December 30, 2011 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," "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
$15,000 (Settlement of NPCC201100223 and NPCC201100224)	Self-Report	In accordance with the Mitigation Plan, NPCC_URE1 implemented a new system for PSP substation access. First, NPCC_URE1 provided documentation that site-specific lock boxes have been installed at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. Second, NPCC_URE1 provided documentation that a new procedure has been created, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. Thus, the general procedure in place for reviewing access lists and revoking substation and PSP access is now in effect in instances in which the card reader system is not functioning.	1/10/2011	3/22/2011	Neither Admits nor Denies	NPCC considered NPCC_URE1's internal compliance program, which was in place at the time of the violation, to be a mitigating factor in the penalty determination.
$15,000 (Settlement of NPCC201100223 and NPCC201100224)	Self-Report	In accordance with the Mitigation Plan, NPCC_URE1 implemented a new system for PSP substation access. First, NPCC_URE1 provided documentation that site-specific lock boxes have been installed at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. Second, NPCC_URE1 provided documentation that a new procedure has been created, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. Thus, the general procedure in place for reviewing access lists and revoking substation and PSP access is now in effect in instances in which the card reader system is not functioning.	1/10/2011	3/22/2011	Neither Admits nor Denies	NPCC considered NPCC_URE1's internal compliance program, which was in place at the time of the violation, to be a mitigating factor in the penalty determination.

Attachment A-2

December 30, 2011 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," "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
$5,000 (Settlement of NPCC201100225 and NPCC201100226	Self-Report	In accordance with the Mitigation Plan, NPCC_URE2 implemented a new system for PSP substation access. First, NPCC_URE2 provided documentation that site-specific lock boxes have been installed at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. Second, NPCC_URE2 provided documentation that a new procedure has been created, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. Thus, the general procedure in place for reviewing access lists and revoking substation and PSP access is now in effect in instances in which the card reader system is not functioning.	1/10/2011	3/22/2011	Neither Admits nor Denies	NPCC considered NPCC_URE2's internal compliance program, which was in place at the time of the violation, to be a mitigating factor in the penalty determination.
$5,000 (Settlement of NPCC201100225 and NPCC201100226	Self-Report	In accordance with the Mitigation Plan, NPCC_URE2 implemented a new system for PSP substation access. First, NPCC_URE2 provided documentation that site-specific lock boxes have been installed at each facility in question, and the old locks associated with the undocumented keys have been removed. Individuals no longer have a physical key to access the substation should the card reader system fail. Second, NPCC_URE2 provided documentation that a new procedure has been created, in which just one key is kept at a separate office in a site-specific lock box with security personnel who are trained in the documented access procedure. Thus, the general procedure in place for	1/10/2011	3/22/2011	Neither Admits nor Denies	NPCC considered NPCC_URE2's internal compliance program, which was in place at the time of the violation, to be a mitigating factor in the penalty determination.

Attachment A-2

December 30, 2011 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," "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
$6,000	Self-Report	Upon discovery of the violation, RFC_URE1 ensured that the access rights of the purchase company's employee who left the computer manufacturer vendor unescorted within the PSP were terminated. The purchase company's has moved its employees and assets, including its data storage servers, out of RFC_URE1's building, ensuring that a similar incident will not be possible in the future. RFC_URE1 disabled any and all purchase company cards that still showed to be "Active."	4/29/2011	6/3/2011	Agrees and Stipulates to the Facts	ReliabilityFirst commends certain aspects of RFC_URE1's compliance program, in effect at the time of the alleged violation, and considered them as mitigating factors.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Spot Check	To mitigate its violation of CIP-003-1 (2) R1.1, SPP RE_URE1 updated its Policy to include the applicable requirements of CIP-002 through CIP-009, Version 3. SPP RE_URE1 trained all affected employees on the updated Policy and documented its training to make certain all affected employees were included in the training.	12/10/2010	1/4/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant 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
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Spot Check	To mitigate its violation of CIP-007-1 R1.3, SPP RE_URE1 took the following mitigating actions: developed a security patch management policy to identify and review all applicable security patches for all devices and Cyber Assets within the Electronic Security Parameter (ESP) within 30 days of their release; amended its policy to include requirements for documenting rationale and any compensating measures for any patches not installed; created a template to use where each new patch is reviewed for consideration; implemented a policy that all reviewed patches should follow the defined template; and trained all affected employees on the patch management policy.	11/12/2010	12/6/2010	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate the violation of CIP-005-1 R1.5, SPP RE_URE1 completed its Mitigation Plans associated with its violations of CIP-003-1 R1, R4, R5, and R6, CIP-005-1 R2 and R3, and CIP-007-1 R1, R3, R5, R6, R8 and R9. SPP RE_URE1 ensured not only that its CCAs are protected pursuant to those requirements, but also that its CAs used in the access control and/or monitoring of its ESP are afforded the same protective measures as required by CIP-005-3 R1.5. Also, SPP RE_URE1 developed a process to ensure that all newly implemented CAs will be afforded the protective measures as required by CIP-005-3 R1.	3/2/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-005-1 R2, SPP RE_URE1 took the following actions: reviewed all of its current firewall configurations for correctness; ensured that all default deny configurations were applied in all of its firewall rules for inbound and outbound communications; documented baseline configurations of all of its firewalls including comments on the use of open ports; reviewed all of its ports and services configurations for correctness; documented baseline configurations of all ports and services including the use for all CCA devices; and developed a procedure associated with ports and service and firewall configurations.	11/4/2010	11/23/2010	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.

Attachment A-2

December 30, 2011 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," "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
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-005-1 R3, SPP RE_URE1 completed the following actions: performed a feasibility assessment for an automated tool to enable security logging and monitoring; created a process for logging security events for access points to the ESP through an automated tool process; developed an updated policy for monitoring the security events through an automated tool or process; and trained all affected SPP RE_URE1 employees on the updated policy.	2/16/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-005-1 R4, SPP RE_URE1 identified the recommendations from its vulnerability assessment and developed and documented action plans to mitigate any vulnerabilities. SPP RE_URE1 developed a written procedure that included the scope of the vulnerability assessment, the steps required for completing the vulnerability assessment, the process for documenting the assessment results, and the process for mitigating the vulnerabilities found during the assessment. Additionally, SPP RE_URE1 developed a template to document the mitigation process for its vulnerability assessments. Finally, SPP RE_URE1 scheduled and performed a Vulnerability Assessment according to its new revised procedure.	2/25/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.

Attachment A-2

December 30, 2011 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," "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
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R2, SPP RE_URE1 reviewed all of its ports and services configurations for correctness and then documented baseline configurations of all ports and services taking into consideration that different ports and services are utilized during emergency situations. With the configurations, SPP RE_URE1 is able to ensure that only the ports and services required for normal and emergency operations are enabled.	11/4/2010	11/23/2010	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R23, SPP RE_URE1 developed a security patch management policy to identify and review all applicable security patches for all CAs within its ESP within 30 days of the patch release. In its revised policy, SPP RE_URE1 included requirements for documenting rationale and any compensating measures for patches that were not installed. SPP RE_URE1 created a template that will be used when a new patch is reviewed for consideration and implemented its security patch management program to follow the defined templates, forms and change systems. Finally, SPP RE_URE1 trained its affected employees on the patch management policy and documented attendance of the training.	11/12/2010	11/23/2010	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.

Attachment A-2

December 30, 2011 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," "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
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R5, SPP RE_URE1 developed a comprehensive list of all shared, default and generic accounts for all CCA devices and the SPP RE_URE1 personnel who have access to those accounts. SPP RE_URE1 developed processes for new shared accounts that are created or deleted and for an annual review to be performed on the list of employees who have access to its CCAs and each employee's privileges. Also, SPP RE_URE1 developed a process to ensure that all security related information is properly logged and maintained. SPP RE_URE1 completed its mitigation of CIP-005-1 R3, which implemented its logging and monitoring system. Finally, SPP RE_URE1 updated the applicable policies to include the revised account management procedures.	2/18/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R6, SPP RE_URE1 performed a feasibility assessment for an automated tool to enable security logging and monitoring. SPP RE_URE1 then implemented the chosen automated tool for logging security events for its CAs within its EMS. A policy for monitoring security events through the automated tool and process was developed and included procedures with detailed requirements for retention of electronic access logs for at least 90 days, and for at least 3 years for security-related incidents. Finally, SPP RE_URE1 trained and documented attendance of training for all employees who are responsible for implementing and following the updated policy and procedures.	2/16/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.

Attachment A-2

December 30, 2011 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," "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
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R8, SPP RE_URE1 identified the recommendations from its Vulnerability Assessment and developed and documented action plans to mitigate any vulnerabilities. SPP RE_URE1 developed a written procedure that included the scope of the vulnerability assessment, the steps required for completing the vulnerability assessment, the process for documenting the assessment results and the process for mitigating the vulnerabilities found during the assessment. Additionally, SPP RE_URE1 developed a template to document the mitigation process for its vulnerability assessments. Finally, SPP RE_URE1 scheduled and performed a Vulnerability Assessment according to its new revised procedure.	2/25/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.
$68,000 (Settlement of SPP201000288, SPP201000289, SPP201000394, SPP201000395. SPP201000396, SPP201000397, SPP201000399, SPP201000340, SPP201000401, SPP201000402, SPP201000403, and SPP201000404)	Self-Certification	To mitigate its violation of CIP-007-1 R9, SPP RE_URE1 completed its Mitigation Plans for CIP-007 R1, R2, R3, R5, R6 and R8 and developed a procedure to review all documents and procedures referenced in CIP-007 at least annually and any changes that result from the review will be documented within 90 calendar days.	2/28/2011	3/17/2011	Does Not Contest	SPP RE_URE1 implemented a formal Internal Compliance Program and SPP RE considered it to be a mitigating factor in determining the penalty amount for the instant violations.

Attachment A-2

December 30, 2011 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," "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
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-005-1 R2. In accordance with the Mitigation Plan, Texas RE_URE1 completed the cyber vulnerability assessment process, ports and services documentation, and review of accounts as required by the Standard. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/27/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-005-1 R2. In accordance with the Mitigation Plan, Texas RE_URE1 completed the cyber vulnerability assessment process, ports and services documentation, and review of accounts as required by the Standard. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/27/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.

Attachment A-2

December 30, 2011 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," "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
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-005-1 R4. In accordance with the Mitigation Plan, Texas RE_URE1 completed the cyber vulnerability assessment process, ports and services documentation, and review of accounts as required by the Standard. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/27/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-005-1 R4. In accordance with the Mitigation Plan, Texas RE_URE1 completed the cyber vulnerability assessment process, ports and services documentation, and review of accounts as required by the Standard. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/27/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.

Attachment A-2

December 30, 2011 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," "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
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R2. In accordance with the Mitigation Plan, Texas RE_URE1 completed documentation for enabling required ports and services, disabling other ports and services, and compensating measures in cases where ports and services cannot be disabled. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R2. In accordance with the Mitigation Plan, Texas RE_URE1 completed documentation for enabling required ports and services, disabling other ports and services, and compensating measures in cases where ports and services cannot be disabled. The procedure document was approved, dated and signed by the authorized senior manager and fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.

Attachment A-2

December 30, 2011 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," "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
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R6. In accordance with the Mitigation Plan, Texas RE_URE1 completed the appropriate monitoring on Cyber Assets within the ESP. The procedure was fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R6. In accordance with the Mitigation Plan, Texas RE_URE1 completed the appropriate monitoring on Cyber Assets within the ESP. The procedure was fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.

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
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R8. In accordance with the Mitigation Plan, Texas RE_URE1 completed its annual cyber vulnerability assessment of all Cyber Assets within the ESP. The procedure was fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.
$10,000 (for TRE202000130, TRE201000132, TRE201000131, TRE202000133, TRE201000227, TRE201000233, TRE201000230, TRE201000236, TRE201000232, and TRE201000238)	Self-Report	Texas RE_URE1 submitted a Mitigation Plan to Texas RE to address the violation of CIP-007-1 R8. In accordance with the Mitigation Plan, Texas RE_URE1 completed its annual cyber vulnerability assessment of all Cyber Assets within the ESP. The procedure was fully implemented by Texas RE_URE1.	1/29/2010	7/20/2011	Neither Admits nor Denies	Texas RE_URE1's compliance program was considered a mitigating factor in the determination of the penalty amount.

Attachment A-2

December 30, 2011 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," "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
$5,600	Self-Report	WECC_URE1 submitted a Mitigation Plan and took the following actions: 1) Reviewed and revised its existing CIP Critical Cyber Asset (CCA) procedures to increase their scope to include the addition of the PACM devices; 2) Utilized the revised procedures to implement each protective measure and documented successful completion of each procedure; 3) Agreed that every PACM device in all four identified classes will undergo all WECC_URE1 CIP procedures related to CIP-005 R2 and R3; CIP-007 R2 to R6 and R8; and CIP-009 R5; and 4) Incorporated all PACM assets used in the access control and monitoring of the PSP, which were previously contained in a separate program, into WECC_URE1's existing program for CCAs.	6/14/2011	11/18/2011	Accepts	WECC_URE1 has an internal compliance program which WECC considered a mitigating factor.

Document Content(s)