



NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

January 31, 2011

Ms. Kimberly 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 Penalty¹ (Administrative Citation NOP) in Attachment A regarding 19 Registered Entities² 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 Administrative Citation NOP resolves 41 violations⁵ of 11 Reliability Standards. In order to be a candidate for inclusion in this initial Administrative Citation NOP, the violations are those that had a minimal impact on the reliability of the bulk power system (BPS). In all cases, the violations contained in these NOP have been mitigated, certified by the respective Registered Entities as mitigated and verified by the Regional Entity as having been mitigated.

Some of the violations at issue in the 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

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 (2010). *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 consists of three excel spreadsheets.

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.

NERC Administrative Citation Notice of Penalty

January 31, 2011

Page 2

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. 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 the violations. While some of the Registered Entities have neither admitted nor denied 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 Administrative Citation NOP resolves 41 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 posed minimal risk to the reliability of the BPS.⁶ Completing these minimal risk 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 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 Board of Trustees Compliance Committee (NERC BOTCC) of the findings and penalties reflected in Attachment A. In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (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 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 Mitigation⁷

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 "parking ticket"-type administrative processes aligned with the significance of the subject violations).

⁷ See 18 C.F.R § 39.7(d)(7).

NERC Administrative Citation Notice of Penalty
January 31, 2011
Page 3

Statement Describing the Proposed Penalty, Sanction or Enforcement Action Imposed⁸

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008 Guidance Order, the October 26, 2009 Guidance Order and the August 27, 2010 Guidance Order,⁹ the NERC BOTCC reviewed the Administrative Citation NOP and the attachments thereto, on January 10, 2011. The NERC BOTCC approved the Administrative Citation Spreadsheet, including the Regional Entities' imposition of financial penalties as reflected in Attachment A, based upon its findings and determinations, the NERC BOTCC's review of the applicable requirements of the Commission-approved Reliability Standards, and the underlying facts and circumstances of the violations at issue.

Pursuant to Order No. 693, the 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.

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.

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).

NERC Administrative Citation Notice of Penalty

January 31, 2011

Page 4

A Form of Notice Suitable for Publication¹⁰

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:

<p>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</p>	<p>Rebecca J. Michael* Assistant General Counsel V. Davis Smith Attorney 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 davis.smith@nerc.net</p>
<p>*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. <i>See also</i> Attachment B for additions to the service list.</p>	

¹⁰ See 18 C.F.R § 39.7(d)(6).

NERC Administrative Citation Notice of Penalty

January 31, 2011

Page 5

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

Rebecca J. Michael
Assistant General Counsel
V. Davis Smith
Attorney
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
davis.smith@nerc.net

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

cc: Entities listed in Attachment B

ATTACHMENT A

JANUARY 2011 ADMINISTRATIVE CITATION NOTICE OF PENALTY

CONSISTING OF

- 1. ATTACHMENT A-1:**
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
NON-CIP VIOLATIONS ONLY

- 2. ATTACHMENT A-2:**
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
PRIVILEGED AND CONFIDENTIAL INFORMATION REMOVED (CIP AND/OR NON-CIP)

- 3. ATTACHMENT A-3:**
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
CONTAINS PRIVILEGED AND CONFIDENTIAL INFORMATION – DO NOT RELEASE (CIP AND/OR NON-CIP)

ATTACHMENT B

**REGIONAL ENTITY SERVICE LIST FOR JANUARY 2011 ADMINISTRATIVE
CITATION NOTICE OF PENALTY**

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 RFC:

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

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

FOR SERC:

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

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

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

FOR SPP RE:

Stacy Dochoda*
General Manager
Southwest Power Pool Regional Entity
16101 La Grande, Ste 103
Little Rock, AR 72223

(501) 688-1730
(501) 821-8726 – facsimile
sdochoda@spp.org

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

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

FOR TEXAS RE:

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

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

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-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 June 27, 2008, 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. The sub-requirements each have Lower VRFs.
- 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.
- 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.
- 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. CIP-004-1 R4 and R4.1 have Lower VRFs.
- 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.

ATTACHMENT D

UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

North American Electric Reliability Corporation

Docket No. NP11-____-000

NOTICE OF FILING
January 31, 2011

Take notice that on January 31, 2011, the North American Electric Reliability Corporation (NERC) filed an Administrative Citation Notice of Penalty regarding nineteen (19) Registered Entities in six (6) 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.2
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
PRIVILEGED AND CONFIDENTIAL INFORMATION
REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	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 Council of Compliance	Adm'd or Non-Adm'd
MRO	MRO_LRE1	NCRXXXX	MRO00000106	MRO_LRE1 self-certified non-compliance with Reliability Standard CIP-004-1, R2 because evidence of cyber security training (CST) was not available for employees pursuant to the Standard. In order to verify the self-certification, MRO conducted a Spot Check. During the Spot Check, MRO_LRE1 provided documentation to MRO. MRO reviewed the 10 individuals that the MRO_LRE1 internal audit found to have missed training. MRO_LRE1 initiated a process change as of October 1, 2009 to ensure that all individuals with authorized cyber and/or unsecured physical access to Critical Cyber Assets (CCAs) had received CST prior to being granted access. MRO compliance staff reviewed a sample of individuals granted CCA access between October 1, 2009 and March 2, 2010. MRO did not observe any instances where the sampled employees had not received the required CST. MRO determined that the violation began on July 1, 2008 when the Standard became mandatory and enforceable and continued until September 30, 2009. MRO_LRE1 implemented a new process to ensure compliance.	SP-004-1	R2	Medium	Lower	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) for the following reasons. These 10 individuals represent less than 1% of the individuals on MRO_LRE1's Access List. Upon learning of the non-compliance through completing an internal audit, MRO_LRE1 initiated a new PRA policy. The new policy requires those employees with authorized cyber and/or unsecured physical access to CCAs to have evidence of the completion of a PRA prior to being granted access to the CCAs. Additionally, MRO staff has not found any additional instances of access being granted without receipt of the CIP Awareness Training subsequent to the implementation of the new policy.	7/1/2008	9/30/2009	\$0	Self-certification	MRO_LRE1 replaced the previous Standard Owner for CIP-004 with a new Director. The Manager of Security issued a physical file folder for each individual who has unsecured physical access and/or authorized electronic access to CCAs. These folders contain all evidence of successful completion of PRA's prior to authorizing the individual's cyber or unsecured physical access to a CCA. MRO_LRE1 personnel verified that the information in the Security file folders matched the information in the physical and electronic access lists and the CIP Personnel List. Security implemented a new policy that ensures the expiration date for an individual's proximity access list will be the earlier of the expiration of the individual's CIP Awareness Training or the expiration of the individual's personal risk assessment (PRA). This ensures that no individual will have unsecured physical access to a CCA facility without (1) authorization, (2) an up-to-date PRA, and (3) annual CIP Awareness Training.	9/31/2009	1/14/2010	Adm'd
MRO	MRO_LRE1	NCRXXXX	MRO00000107	MRO_LRE1 self-certified non-compliance with Reliability Standard CIP-004-1, R3 because evidence of cyber security training (CST) was not available for employees pursuant to the Standard. In order to verify the self-certification, MRO conducted a Spot Check. During the Spot Check, MRO_LRE1 provided documentation to MRO. MRO reviewed the 10 individuals that the MRO_LRE1 internal audit found to be missing PRA's. MRO_LRE1 initiated a process change as of October 1, 2009 to ensure that all individuals with authorized cyber and/or unsecured physical access to CCAs have undergone a PRA prior to being granted access. MRO compliance staff reviewed a sample of individuals granted CCA access between October 1, 2009 and March 2, 2010. MRO did not observe any instances where the sampled employees had not undergone a PRA within 30 days of being granted access to CCAs. MRO determined that the violation began on July 1, 2008 when the Standard became mandatory and enforceable and continued until September 30, 2009.	SP-004-1	R3	Lower	High	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) for the following reasons. These 10 individuals represent less than 1% of the individuals on MRO_LRE1's Access List. Upon learning of the non-compliance through completing an internal audit, MRO_LRE1 initiated a new PRA policy. The new policy requires those employees with authorized cyber and/or unsecured physical access to CCAs to have evidence of the completion of a PRA prior to being granted access to the CCAs. Additionally, MRO staff has not found any additional instances of access being granted without receipt of the CIP Awareness Training subsequent to the implementation of the new policy.	7/1/2008	9/30/2009	\$0	Self-certification	MRO_LRE1 replaced the previous Standard Owner for CIP-004 with a new Director. The Manager of Security issued a physical file folder for each individual who has unsecured physical access and/or authorized electronic access to CCAs. These folders contain all evidence of successful completion of PRA's prior to authorizing the individual's cyber or unsecured physical access to a CCA. MRO_LRE1 personnel verified that the information in the Security file folders matched the information in the physical and electronic access lists and the CIP Personnel List. Security implemented a new policy that ensures the expiration date for an individual's proximity access list will be the earlier of the expiration of the individual's CIP Awareness Training or the expiration of the individual's PRA. This ensures that no individual will have unsecured physical access to a CCA facility without (1) authorization, (2) an up-to-date PRA, and (3) annual CIP Awareness Training.	9/31/2009	1/14/2010	Adm'd
MRO	MRO_LRE1	NCRXXXX	MRO00000108	MRO_LRE1 self-certified non-compliance with Reliability Standard CIP-004-1, R4 because it did not have sufficient documentation supporting that it had updated its NERC CIP Personnel List (Access List) when the required 7 day or 24 hour time frame for certain individuals who no longer required cyber or unsecured physical access to Critical Cyber Assets (CCAs). In order to verify the self-certification of non-compliance, MRO conducted a Spot Check. During the Spot Check, MRO_LRE1 provided documentation to MRO. MRO reviewed the 10 individuals that the MRO_LRE1 internal audit found to be missing PRA's. MRO_LRE1 initiated a process change as of October 1, 2009 to ensure that all individuals with authorized cyber and/or unsecured physical access to CCAs have undergone a PRA prior to being granted access. MRO compliance staff reviewed a sample of individuals granted CCA access between October 1, 2009 and March 2, 2010. MRO did not observe any instances where the sampled employees had not undergone a PRA within 30 days of being granted access to CCAs. MRO determined that the violation began on July 1, 2008 when the Standard became mandatory and enforceable and continued until September 30, 2009.	SP-004-1	R4	Lower	Severe	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) for the following reasons. With regard to the 3 individuals whose access was not reviewed within 7 days of no longer requiring access, these individuals' primary work facility included a terminal for MRO_LRE1's Energy Management System. On January 22, 2009, the terminal was removed from the facility and the individuals could no longer physically or electronically access the CCA. Although the Access List was not updated within 7 days, the individuals' no longer required access to the ability to access the CCA. For the 1 individual terminated for cause, MRO_LRE1 has no additional documentation supporting the date that the individual was notified as inactive in the NERC CIP Personnel List, a screenshot of MRO_LRE1's Energy Management System demonstrates that the individual's access card expired on January 16, 2009, the date of termination, and was last used on November 19, 2008.	7/1/2008	9/30/2009	\$0	Self-certification	MRO_LRE1 replaced the previous Standard Owner for CIP-004 with a new Director. MRO_LRE1 initiated a process to ensure that all Security personnel the sign-in policy for logs, including logs for physical access to Critical Cyber Assets (CCAs). The Manager of Security issued a physical folder for each individual who has unsecured physical access and/or authorized electronic access to a CCA. These folders contain all documentation that supports MRO_LRE1's compliance with the requirements of CIP-004. MRO_LRE1 personnel verified that the information in the Security file folders matched the information in the physical and electronic access lists and the CIP Personnel List. Security implemented a new policy that ensures the expiration date for an individual's proximity access list will be the earlier of the expiration of the individual's CIP Awareness Training or the expiration of the individual's PRA. This ensures that no individual will have unsecured physical access to a CCA facility without (1) authorization, (2) an up-to-date PRA, and (3) annual CIP Awareness Training. The access will be automatically reviewed by the MRO_LRE1 system. MRO_LRE1's Security and human resources	9/31/2009	1/14/2010	Adm'd
MRO	MRO_LRE2	NCRXXXX	MRO00100219	MRO conducted an on-site CIP Spot Check of MRO_LRE2. MRO determined that MRO_LRE2 has documented and implemented a Cyber Security Policy. The Cyber Security Policy addresses requirements in CIP-002 through CIP-009, including emergency response. Although MRO_LRE2 makes its Cyber Security Policy readily available to all employees based on their job function via the company intranet, MRO_LRE2 has not maintained evidence sufficient to confirm that the MRO_LRE2 Cyber Security Policy was made readily available to contract SCADA vendor personnel.	SP-003-1	R1	Lower	Severe	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although there was no evidence that the SCADA vendor personnel were provided access to the MRO_LRE2 Cyber Security Policy, they were easily monitored by MRO_LRE2 while on-site and during remote interactive troubleshooting sessions.	7/1/2008	12/31/2009	\$0	Spot Check	MRO_LRE2 mitigated the violation upon development and implementation of a revised risk-based methodology for determination of Critical Assets. MRO_LRE2 first implemented its risk-based methodology with an effective date of June 8, 2007. Based on an understanding resulting from continuing self-education on the intent and requirements of the CIP standards, MRO_LRE2 decided to re-evaluate its assessment methodology. This decision was supported by recommendations received by consultants hired to assist MRO_LRE2 in assessing its audit readiness. In assessing the criticality of MRO_LRE2's assets to the safe and reliable operation of the BPS, impact criteria were examined and each of MRO_LRE2's assets analyzed against that criteria. These criteria were aimed at gaining an industry knowledge gathered through NERC and MRO educational offerings, comparison to the efforts of similar utilities, and input from engineering consultants. In applying its revised risk-based methodology, based on the data collected and input by MRO_LRE2 into the assessment, MRO_LRE2 determined that it does not have any Critical Assets. MRO_LRE2 implemented its revised methodology.	9/31/2009	12/10/2010	Adm'd
MRO	MRO_LRE2	NCRXXXX	MRO00100220	During an on-site CIP Spot Check, MRO determined that MRO_LRE2 has established, documented and maintained a Risk-Based Methodology (RBM) for self-certification for compliance to CIP-004. MRO_LRE2 conducted an internal Risk-Based Methodology (RBM) assessment that MRO_LRE2 has not maintained evidence sufficient to confirm that annual training is provided to all employees. Specifically, SCADA vendor personnel, as required by Requirement 2.3, MRO_LRE2 failed to provide any training records for its SCADA vendor personnel.	SP-004-1	R2	Medium	Lower	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although there was no evidence that the SCADA vendor personnel received cyber security training from MRO_LRE2, they were easily monitored by MRO_LRE2 while on-site and during remote interactive troubleshooting sessions. MRO did not segregate the penalty in this case based on the violation was outside of the applicable report period.	7/1/2008	12/31/2009	\$0	Spot Check	MRO_LRE2 mitigated the violation upon development and implementation of a revised risk-based methodology for determination of Critical Assets. MRO_LRE2 first implemented its risk-based methodology with an effective date of June 8, 2007. Based on an understanding resulting from continuing self-education on the intent and requirements of the CIP standards, MRO_LRE2 decided to re-evaluate its assessment methodology. This decision was supported by recommendations received by consultants hired to assist MRO_LRE2 in assessing its audit readiness. In assessing the criticality of MRO_LRE2's assets to the safe and reliable operation of the BPS, impact criteria were examined and each of MRO_LRE2's assets analyzed against that criteria. These criteria were aimed at gaining an industry knowledge gathered through NERC and MRO educational offerings, comparison to the efforts of similar utilities, and input from engineering consultants. In applying its revised risk-based methodology, based on the data collected and input by MRO_LRE2 into the assessment, MRO_LRE2 determined that it does not have any Critical Assets. MRO_LRE2 implemented its revised methodology.	9/31/2009	12/10/2010	Adm'd
MRO	MRO_LRE2	NCRXXXX	MRO00100221	During an on-site CIP Spot Check, MRO determined that MRO_LRE2 has not maintained evidence sufficient to show proper access list maintenance on the contractor granted access to MRO_LRE2's systems as mandated by Requirement R1.1. MRO_LRE2 did not include its SCADA vendor personnel.	SP-004-1	R4	Lower	Lower	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although there was no evidence that the SCADA vendor personnel were provided access to the MRO_LRE2 Cyber Security Policy, they were easily monitored by MRO_LRE2 while on-site and during remote interactive troubleshooting sessions.	7/1/2008	12/31/2009	\$0	Spot Check	MRO_LRE2 mitigated the violation upon development and implementation of a revised risk-based methodology for determination of Critical Assets. MRO_LRE2 first implemented its risk-based methodology with an effective date of June 8, 2007. Based on an understanding resulting from continuing self-education on the intent and requirements of the CIP standards, MRO_LRE2 decided to re-evaluate its assessment methodology. This decision was supported by recommendations received by consultants hired to assist MRO_LRE2 in assessing its audit readiness. In assessing the criticality of MRO_LRE2's assets to the safe and reliable operation of the BPS, impact criteria were examined and each of MRO_LRE2's assets analyzed against that criteria. These criteria were aimed at gaining an industry knowledge gathered through NERC and MRO educational offerings, comparison to the efforts of similar utilities, and input from engineering consultants. In applying its revised risk-based methodology, based on the data collected and input by MRO_LRE2 into the assessment, MRO_LRE2 determined that it does not have any Critical Assets. MRO_LRE2 implemented its revised methodology.	9/31/2009	12/10/2010	Adm'd
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100131	In 2008, NPCC_LRE1 implemented the annual cyber security training program as part of its overall compliance assessment. As part of the preparation for self-certification for compliance to CIP-004, NPCC_LRE1 conducted an internal Risk-Based Methodology (RBM) assessment that NPCC_LRE1 has not maintained evidence sufficient to confirm that annual training is provided to all employees. Specifically, SCADA vendor personnel, as required by Requirement 2.3, NPCC_LRE1 failed to provide any training records for its SCADA vendor personnel.	SP-004-1	R2.3	Lower	High	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although there was no evidence that the SCADA vendor personnel received cyber security training from NPCC_LRE1, they were easily monitored by NPCC_LRE1 while on-site and during remote interactive troubleshooting sessions. MRO did not segregate the penalty in this case based on the violation was outside of the applicable report period.	7/1/2010	4/30/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 reviewed all individuals with authorized cyber and unsecured physical access to CCAs. Validated that all individuals with authorized cyber and unsecured physical access to CCAs have received the required training. 3. Provided training to 20 personnel identified as lacking the training or the necessary evidence demonstrating the training was taken. 4. Implemented system access to ensure no individual with authorized cyber and unsecured physical access to CCAs has access to the system without having received the required training. 5. Updated the Access List to reflect the training records for all individuals with authorized cyber and unsecured physical access to CCAs. 6. Updated the Access List to reflect the training records for all individuals with authorized cyber and unsecured physical access to CCAs. 7. Enhanced the sign-in attendance sheets for group viewing of training to be prepared and reviewed by the Human Resource staff. 8. Communicated any training procedure changes to all training representatives for new and continuing access and to prevent recurrence. 9. Implemented any training procedure changes to all training representatives for new and continuing access and to prevent recurrence.	9/30/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100132	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the generation ratings methodology. 2. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Lower	Lower	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	4/30/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 reviewed the specific elements and criteria required by FAC-008-1 to be addressed for generation facility ratings to the point of interconnection with the generation facilities. 2. Revised existing generation facility rating methodology to ensure that all required elements and criteria are addressed. 3. Revised and updated the generation facility rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Conducted training to communicate all procedural changes contained in the revised generation facility rating methodology.	9/30/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100133	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Lower	Lower	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	4/30/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 reviewed the specific elements and criteria required by FAC-008-1 to be addressed for transmission facility ratings to the point of interconnection with the generation facilities. 2. Revised existing transmission facility rating methodology to ensure that all required elements and criteria are addressed. 3. Revised and updated the transmission facility rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Conducted training to communicate all procedural changes contained in the revised transmission facility rating methodology.	9/30/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100134	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 4. Performed an audit of all elements to determine the most limiting element for each regulated NPCC_LRE1 Generating facility. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Generator Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100135	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 3. Incorporated existing design rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Transmission Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100136	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 3. Incorporated existing design rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Transmission Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100137	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 3. Incorporated existing design rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Transmission Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100138	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 3. Incorporated existing design rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Transmission Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100139	As part of NPCC_LRE1's overall compliance program, an enhanced evaluation of NPCC_LRE1's program materials was conducted as a result of recent industry compliance actions which led to the identification of the following potential gaps: 1. NPCC_LRE1's existing rating methodology did not specifically take into account the complete scope of elements contained in Requirement 1.1, specifically relay protective devices, and series and short compensating devices.	FAC-008-1	R1	Medium	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because NPCC_LRE1 had an existing rating methodology document, but did not specifically take into account the generation ratings methodology. NPCC_LRE1 documentation needed to be reviewed and revised to ensure that all required elements and criteria were met for generators and associated equipment as to the point of interconnection with the transmission system. NPCC_LRE1 also performed a complete review of its existing transmission and generation rating methodology documents and determined that they needed to be updated to cite relay protective devices and series and short compensation devices. These documents are used for developing facility ratings and, as such, NPCC_LRE1 had documentation in place to perform this task, but needed attention to incorporate all applicable equipment and provide individual documentation for transmission and generation facility rating methodology.	02/15/2007	7/15/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 assembled a list of missing transmission elements which were added in NPCC_LRE1's revised Transmission Facility Ratings Methodology under FAC-008-1 for transmission lines and associated transmission elements. 3. Established a procedure to communicate all Transmission Facility Ratings. 3. Incorporated existing design rating methodology to address additional elements specifically components resulting from the transmission element gathering/verification process. 4. Approved and issued the Generator Facility Ratings book. 5. Conducted training to communicate all procedural changes necessary to maintain the Transmission Facility Ratings book.	7/15/2010	12/20/2010	Neither Adm'd nor Denies
NPCC	NPCC_LRE1	NCRXXXX	NPCC20100153	During NPCC_LRE1's preliminary 2010 Quarterly review process, it was determined that 3 employees with unsecured physical access to Critical Cyber Assets (CCAs) were found to have personal risk assessments (PRAs) that had not been updated when the surveyary requirement.	SP-004-1	R3	Lower	Moderate	NPCC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although there was no evidence that the SCADA vendor personnel received cyber security training from NPCC_LRE1, they were easily monitored by NPCC_LRE1 while on-site and during remote interactive troubleshooting sessions. MRO did not segregate the penalty in this case based on the violation was outside of the applicable report period. It should also be noted that the required PRA for these 3 employees resulted in no clearance issues or adverse results.	1/1/2010	4/30/2010	\$5,000 total penalty for NPCC20100132, NPCC20100133, NPCC20100134, NPCC20100135, NPCC20100136, NPCC20100137, NPCC20100138, NPCC20100139	Self-report	NPCC_LRE1 reviewed and validated the dates of the PRAs for all employees with authorized cyber and unsecured physical access to Critical Cyber Assets. 2. Revised cyber and physical unsecured physical access for the 3 employees whose PRAs had not been updated within the required seven-year period. 3. Performed an audit of all employees whose PRAs had not been updated within the required seven-year period. 4. Reviewed and reaffirmed the existing procedures, as necessary, to ensure that PRAs are performed for all employees with authorized cyber and unsecured physical access to CCAs every seven years.	9/30/2010	12/20/2010	Neither Adm'd nor Denies
SPP	SPP_LRE1	NCRXXXX	SPP20100135	On June 30, 2010 SPP_LRE1 submitted a Self-Report of a violation of SP-003-1. During an internal compliance assessment, SPP_LRE1 discovered that while it has tested backup devices on its servers, SPP_LRE1 Energy Management System (EMS) staff indicated that they have never tested the other backup media devices (media switches) on Critical Cyber Assets (CCAs) and did not have evidence of such tests.	SP-003-1	R5	Lower	Severe	SPP_LRE1 has documented that SPP_LRE1's violation of SP-003-1, R5. SPP_LRE1 failed to test its backup media devices for some of its CCAs. SPP_LRE1 was testing its EMS Server backup devices.	7/1/2009	7/31/2010	\$0	Self-report	SPP_LRE1 has been testing media devices as of July 23, 2010.	7/23/2010	12/10/2010	Neither Adm'd nor Denies
SPP	SPP_LRE1	NCRXXXX	SPP20100160	SPP_LRE1 has been instructed to verify that it conducted a personal risk assessment (PRA) within thirty days of granting authorized unsecured physical access to a Critical Cyber Asset (CCA). The first instance was discovered during SPP_LRE1's October 21, 2009 internal compliance assessment, and was reported to SPP_LRE1 on an October 29, 2009 Self-Report. Specifically, SPP_LRE1 granted an employee unsecured physical access to its dispatch area, a designated CCA, on August 25, 2009, but did not conduct the employee's PRA until October 7, 2009, which was three days after the referenced Reliability Standard's thirty-day deadline had expired. The second instance was discovered during a Spot Check. SPP_LRE1 found that SPP_LRE1 granted another employee unsecured physical access to the dispatch area on August 2, 2009, but did not conduct the employee's PRA until October 7, 2009, which was twelve days after the referenced Reliability Standard's thirty-day deadline had expired.	SP-004-1	R3	Medium	Moderate	SPP_LRE1 has documented that SPP_LRE1's violation of CIP-004-1, R3 posed a minimal risk to the reliability of the bulk power system (BPS) for the first instance. The employee received the required cyber security training on the date they were granted access, and they had physical access to only one CCA (the dispatch area). Because the dispatch area is staffed twenty-four hours a day, seven days a week, there was some supervision and oversight by other personnel working in this area during the violation period.	9/15/2009	10/7/2009	\$0	Self-report for first instance; Spot Check for second instance	The violation was mitigated when SPP_LRE1 conducted PRA's for both employees on October 7, 2009. To help ensure future compliance with CIP-004-1, R3, SPP_LRE1 revised its Cyber Security Policy on October 8, 2009, to require PRA's to be conducted prior to granting authorized cyber or unsecured physical access to CCAs.	9/15/2009	9/13/2009	Neither Adm'd nor Denies
SPP	SPP_LRE1	NCRXXXX	SPP20100164	During a Spot Check, SPP_LRE1 determined that SPP_LRE1 was not in compliance with CIP-003-1 R1.1 and R1.2. Regarding R1.1, SPP_LRE1's Cyber Security Policy (CSP) did not address all of the requirements of CIP-003 through CIP-009. The Policy failed to include provisions addressing (i) emergency situations (CIP-003 R1.1.1); (ii) the required annual assessment, documentation, and implementation of an action plan to remediate deficiencies in SPP_LRE1's Critical Cyber Assets (CCAs) Information Protection Program (CIP-003 R1.2.3); (iii) the required annual assessment and documentation of the process for controlling access													

Attachment A-2
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
PRIVILEGED AND CONFIDENTIAL INFORMATION
REMOVED (CIP AND/OR NON-CIP)

Region	Registered Entity	NCR_ID	NERC Violation ID #	Description of the Violation	Reliability Standard	Req. (1,2, 7,8)	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	Admit or Neither Admit or Denies
SPP	SPP_LRE1	NCRXXXX	SPP20090192	During a Spot Check, SPP RE found SPP_LRE1 to be in violation of CIP-008-1 R1.2 and R1.6. Regarding R1.2, although SPP_LRE1's Incident Response Plan included roles and responsibilities of the response team members as required by CIP-008-1 R1.2, the plan did not include the incident handling procedures to be followed in the event of an incident. Regarding R1.6, the incident response testing conducted by SPP_LRE1 did not satisfy the requirements of the Standard. For example, SPP_LRE1's 2008 incident response testing included instruction regarding the procedures in completing the reporting form; however, the testing failed to include a reporting event to involve the incident response team to work through the response plan steps. Additionally, SPP_LRE1's 2009 incident response testing failed to include triggering events to involve the response plan, assemble the incident response team, characterize and classify the event as a reportable incident as required by CIP-008-1 R1.1, and to report an incident that was determined to be reportable to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC).	SPP-008-1	R1 (1,2, 7,8)	Lower	High	SPP RE has determined that SPP_LRE1's violation of CIP-008-1 R1.2 posed a minimal risk to the reliability of the bulk power system (BPS). SPP_LRE1 had an Incident Response Plan in place, even though it lacked specific handling procedures and was not properly tested. The identified incident response team is well established in the support of the CCAAs and would be expected to identify, contain, and ultimately recover from an incident. Further, there have been no reported cyber security incidents to date and therefore the actual impact was minimal.	7/1/2008	8/19/2010	\$500	Spot Check	SPP_LRE1 revised its Incident Reporting and Response Plan to include incident handling and communication procedures. SPP_LRE1 also developed formal cyber security response procedures with specific actions to be taken in response to events that would involve the incident recovery plan. Furthermore, SPP_LRE1's most recent incident response testing included triggering events to involve the response plan, assemble the incident response team, characterize and classify the event as a reportable incident, and to report an incident that was determined to be reportable to the ES-ISAC.	8/19/2010	8/20/10	Neither Admits nor Denies
SPP	SPP_LRE1	NCRXXXX	SPP20090194	During a Spot Check, SPP RE determined that SPP_LRE1 was not in compliance with CIP-008-1 R2 because it failed to test its recovery plans by the required date of compliance (July 1, 2008).	SPP-008-1	R2	Lower	Severe	SPP RE has determined that SPP_LRE1's violation of CIP-008-1 R2 posed a minimal risk to the reliability of the bulk power system (BPS). SPP_LRE1 did have a recovery plan in place, even though it was not tested until seven months beyond the required date of compliance. Further, the entity's support staff is very experienced in the support of the Critical Cyber Assets and can be reasonably expected to perform the appropriate recovery steps for a wide variety of incidents.	7/1/2008	1/28/09	\$700	Spot Check	The violation of CIP-008-1 R2 was mitigated when SPP_LRE1 tested its recovery plans on January 28, 2009, prior to the Spot Check.	2/8/2009	3/7/2010	Neither Admits nor Denies
SPP	SPP_LRE2	NCRXXXX	SPP20090192	On November 16, 2008, SPP_LRE2 submitted a Self Report for a violation of CIP-004-1 RA.1 and RA.2. Regarding RA.1, although quarterly reviews of physical access logs of those personnel with authorized unescorted physical access to Critical Cyber Assets were conducted, the reviews did not include evaluations of each individual to confirm a continued need to have such access. Regarding RA.2, physical access was not restricted within seven days from last date of employment for a retiring employee. Additionally, physical access of 2 employees was not restricted within seven days for 2 employees who failed to complete the required annual cyber security training within the time specified by SPP_LRE2's NERC CIP Cyber Security Policy.	SPP-004-1	RA.1, 4.2	Medium	Lower	SPP RE has determined that SPP_LRE2's violation of CIP-004-1 RA.1 posed a minimal risk to the reliability of the bulk power system (BPS). Regarding RA.1, physical access logs were being reviewed quarterly and would have identified any employees that would have been terminated. An internal review confirmed that no employees with access should have had their access revoked. Regarding RA.2, 1 of the 3 employees was a retiree and did not have access to the facility and made no attempt to gain access. The other 2 employees had previously completed the required training but failed to complete the annual training by SPP_LRE2's deadline; their access was revoked approximately two weeks later. Neither employee attempted to gain access.	7/1/2008	5/11/2010	\$0	Self-report	Regarding RA.1, SPP_LRE2's quarterly reviews of its access logs now include evaluations of each individual to confirm a continued need to have such access. Regarding RA.2, a manual log is now being used to document when physical access is revoked within the time frames required by the Standard. Management, human resources, and facilities training have been conducted to ensure compliance with the Standard. Additionally, the annual NERC CIP Security training was provided well in advance of the deadline to allow adequate time to complete the cross checks of those required to complete the training.	5/11/2010	5/18/2010	Neither Admits nor Denies
MRO	MRO_LRE3	NCRXXXX	MRO20100223	MRO_LRE3 reported that on August 24, 2010, a MRO_LRE3 technician disabled cyber access to an Electronic Security Perimeter (ESP) for a summer team and indicated that a system alarm did not get sent as anticipated. After conducting an internal review, MRO_LRE3 determined that 80 days of the system event logs for 4 newly configured domain servers, which are Critical Cyber Assets (CCAs), had not been maintained as required. MRO_LRE3 transferred from using software called QP to monitor system event logs to using a new Windows Event Collector Service available in Windows Server 2008 Operating System. On June 29, 2010, MRO_LRE3 moved 4 new domain servers with Microsoft Operating System 2008 R2 into the production system. On July 2, 2010, the transition from existing domain servers to new domain servers was complete. On July 13, 2010, when the operating system for the 4 domain servers was upgraded to Windows Server 2008, and the ports/services were migrated, the Windows Event Collector Service was allowed to run, but the Windows Remote Manager Service was disabled. The MRO_LRE3	SPP-007-2	R6	Lower	High	MRO found that the violation posed a minimal risk to the reliability of the bulk power system because although logging facilities/services were not installed during the non-compliant period, the entity was continuously monitoring access to the physical and cyber access points to the ESP, including the domain servers, in real time. System Manager actively checked all servers within the ESP during this period. Also, a daily scan would generate alerts for any ports and services running on CCA servers that were not configured as allowed in System Manager. Any time a change is made on a CCA server, the authorized employee making the change is required to run a port/service scan on the relevant server to ensure the change did not introduce a new port or service. Network administrators would then analyze any unexpected. Access to the subject domain controllers was available only to a small set of restricted access individuals. MRO_LRE3 reported that there were very few administrative changes required during the timeframe when logs were not being properly maintained. On August 31, 2010, a physical scan of 80 days of logs are reinstated.	7/13/2010	12/8/2010	\$0	Self-report	MRO_LRE3 completed the following actions to mitigate the violation: 1. On August 23, 2010 the WERM service was activated on all 4 of the domain controller servers. 2. On August 24, 2010 the Event Collector and WERM services were set up as required services in the System Manager application. The System Manager tool checks every morning to ensure the services are running for all relevant servers and will alert the EMMS tools if these services are not running. 3. On August 24, 2010 the security logs for the last 3 days (August 22 to August 24, 2010) were manually inspected and all expected. The only issue found was the disabling of the item network access. 4. On August 25, 2010 the size of the security event logs were increased to allow for a larger timeframe to be retained. 5. From August 23 to August 28, 2010, the changes implemented were being watched daily and confirmation was made that things were working as expected. 6. On August 31, 2010 changes were made to Windows Group Policy to ensure the WERM and Event Collector Services are enabled. Additional Corrective Taken: 1. All current EMMS tools were provided training on this dependency on August 25, 2010 and September 29,	2/8/2010	12/10/2010	Admits

Attachment A1
January 31, 2011 Public Administrative Citation Notice of Penalty Spreadsheet
NON-CIP VIOLATIONS ONLY

Region	Registered Entity	NCR_ID	NERC Violation ID #	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	Adm'd or Neither Adm'd nor Denied?
MRO	Minnesota Power Cooperative (MPC)	NCR01013	MRO020100026	MPC self-reported on October 13, 2010 that it did not have procedures for the use of Capacity Benefit Margin (CBM). The entity, as a transmission provider, is required to create and post an Open Access Transmission Tariff (OATT) to a public website in order to comply with FERC Order 888. FERC Order 888 requires that all transmission providers must allow access to all of their transmission systems as part of an open access transmission system (OATS) exchange. The OATT is used to publicly post the cost of using the entity's transmission system for "normal" firm energy and ancillary services (such as reserves). It is also used as a reference as to how a transmission provider calculates the Available Transmission Capacity (ATC) which is required for open market trading. Capacity Benefit Margin (CBM) for each transmission provider must be known in order for the ATC calculation to be correct. If a transmission provider's CBM is unknown and reserves are needed by the LSE, then the market makers may be delayed and the energy required for emergency purposes may not be readily available. MPC updated its	MRO-006-1	R1	Lower	Severe	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because MPC does not have any Network Customers under its tariff. Therefore there would be no reliance on CBM. Further, there are no changes needed to the ATC calculation because of CBM.	9/13/2009	6/30/2010	\$0	Self-report	MPC mitigated this issue by updating its OATT to include procedures for the use of CBM on September 28, 2010. The documentation of MPC's use of CBM can be found in Attachment C of that document. The OATT can be found on MPC's website by navigating to http://www.mnpower.com , selecting "Transmission Documents" and opening the "Open Access Transmission Tariff" document.	10/26/2010	10/26/2010	Adm'd
MRO	Minnesota Power Cooperative (MPC)	NCR01013	MRO020100027	MPC self-reported on October 13, 2010 that it did not have procedures for the use of CBM and that it had no procedures posted to website. The entity, as a transmission provider, is required to create and post an OATT to a public website in order to comply with FERC Order 888. MRO-006 became effective on May 19, 2009, and MPC posted its tariff to include procedures on the use of CBM on October 4, 2010.	MRO-006-1	R2	Lower	Severe	MRO determined that the violation posed a minimal risk to BPS reliability because MPC does not have any Network Customers under its tariff. Therefore there would be no reliance on CBM. Further, there are no changes needed to the ATC calculation because of CBM.	9/13/2009	10/04/2010	\$0	Self-report	MPC mitigated this issue by posting its updated OATT to the MPC website. The documentation of MPC's use of CBM can be found in Attachment C of that document. The OATT can be found on MPC's website by navigating to http://www.mnpower.com , selecting "Transmission Documents" and opening the "Open Access Transmission Tariff" document.	10/26/2010	10/26/2010	Adm'd
MRO	Wicorrest Public Service Corporation (WSPC)	NCR00662	MRO020100024	On August 26, 2010, WSPC self-reported a violation of UAR-000-11a, R3.1 because it failed to notify its associated Transmission Operator (TO) within 10 minutes of a status change on automatic voltage regulator (AVR) for Weston 1 plant. Additionally, subsequent to filing the self-report, WSPC discovered that other AVR issues with the Crane Creek and West 1 plant. One instance began on February 4, 2010 and was corrected on September 28, 2010, and another instance began on October 20, 2010 and lasted 24 seconds.	UAR-000-11a	R3	Medium	Severe	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because although the AVR was not in automatic control for the Weston 1 plant, the WSPC system operators maintained the Weston 1 plant in manual control. Additionally, although the Weston 1 plant is connected to a 345 kV line which feeds into Milwaukee, the Weston 3 plant, used as a reserve, is 50 MW, and also connected to the system and was providing automatic voltage regulation. Furthermore, the Crane Creek and West 1 is a 69 MW facility located in a rural setting near Riceville, Iowa. MRO also considered the line and location of the facilities.	2/4/2010	10/22/2010	\$0	Self-report	WSPC Unit 1 (August 6, 2010 event) 1. All WSPC generators capable of operation with a reserve exciter were identified. These units included BPS assets Weston 2, Pullman R, and Pullman B. Completed on August 17, 2010; 2. A training memo was released to plant operators of units capable of reserve exciter operation detailing the requirement to immediately notify the WSPC System Operator Supervisor of reserve exciter operation. Completed on August 24, 2010; 3. Operating procedures for units capable of reserve exciter operation were reviewed and updated to reflect reserve exciter capabilities and a need to notify WSPC System Operator prior to operation with the reserve exciter in service; 4. Procedure GEN-012 was revised to incorporate a clear procedural step requiring the plant operator to notify the WSPC System Operator prior to placing a reserve exciter in service. A corresponding change to the "Voltage AVR Control Log" was made to reflect a reserve exciter notification. Completed on October 4, 2010; 5. Crane Creek Facility was a through September 28, 2010 event; 6. Upon identification, the AVR control was enabled. Completed September 28, 2010; 6. New status alarms for the Crane Creek Site were created. Completed October 20, 2010 event; 7. Upon discovery, the Transmission Operator (TO) was notified. (November 1, 2010); 8. On November 2, 2010, this event was reviewed.	11/19/2010	12/10/2010	Adm'd
MRO	Midstate Power and Water (MPW)	NCR00967	MRO020100016	During an on-site audit conducted April 1-15, 2010, MPW provided the requested maintenance and testing records for the LPLS equipment, the relay, DC circuitry, PTA, and batteries. The MPW maintenance and testing records for the relay, DC circuitry and PTA's equipment these components were maintained and tested under the MPW program. MPW also provided evidence of screen display of SCADA monitoring of PTA's tied to the LPLS relays. MPW conducts battery maintenance and testing on a monthly cycle. The hydrometer used by MPW was out of service for repairs and cannot hydrometer readings were conducted. MRO Auditors concluded that: 1. The Pine Substation batteries had not been tested since June 1, 2009 and were due January 1, 2010; 2. The Pine Substation batteries had not been tested since May 12, 2009 and were due December 12, 2009.	PRC-009-0	R2	Medium	Lower	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) since MPW owns and operates a total underfrequency load shed program of 40 MW. MPW is interconnected with Midwest Energy and MidAmerican Energy via 23 miles of 161 kV transmission lines. Given that MPW may fail to shed more than 40 MW of LPLS load and its local MidAmerican Energy and MidAmerican Energy failure of any part of MPW's LPLS program would be a no impact to the BPS.	12/10/2009	4/22/2010	\$0	Audit	The specific grant testing for these Station batteries was completed on April 26, 2010, using a manual hydrometer. MPW purchased a new Digital Hydrometer to replace the damaged unit on April 16, 2010.	6/25/2010	12/10/2010	Adm'd
MRO	Montana Dakota Utilities (MDU)	NCR01015	MRO020100023	During an on-site audit conducted July 19-29, 2010, MRO determined that the Facility Ratings Methodology document which is the basis for the entire audit period did not address series and shunt compensation devices. MDU mitigated the deficiency by the audit team was on site, and the team reviewed the new document which now identifies the rating methodology to be used for series and shunt compensation devices.	FAC-009-0	R1	Lower	Severe	MRO determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because it is a documentation issue. Additionally, MDU does not have any series compensation devices on its system. MDU has a shunt device used as a reserve. Although the shunt device ratings were provided to the Midwest ISO, despite not being documented in MDU's Facility Ratings Methodology.	9/19/2007	7/28/2010	\$0	Audit	Montana Dakota mitigated the deficiency in its Facility Ratings Methodology while the MRO auditors were on site. Series and shunt compensation devices were identified in version 6.0 dated July 28, 2010, of the Facility Rating Methodology document.	7/28/2010	7/28/2010	Adm'd
NPCC	M. Tom Generating Co., LLC (M. Tom)	NCR10060	NPCC0100016	During an internal audit, it was determined the M. Tom did not have a contact number for the FBI.	CIP-001-1	R4	Medium	Lower	NPCC determined that this violation posed a minimal risk to the reliability of the bulk power system (BPS). M. Tom had been operating under its Internal Procedures on Security, which specifically included requirements for reporting suspected incidents of sabotage to Homeland Security and the Federal Bureau of Investigation (FBI). M. Tom subsequently obtained the contact information and updated its procedures.	6/23/2007	5/7/2010	\$0	Self-report	M. Tom established and documented its contact information with the FBI.	6/5/2010	11/17/2010	Neither Adm'd nor Denied
ERC	Buckeye Power, Inc.	NCR02030	ERC020100012	Buckeye Power self-reported that it was non-compliant with CIP-001-1, R4 for a period of approximately three months, between June 18, 2007 and September 11, 2007. Buckeye Power did not have a documented FBI contact during that period.	CIP-001-1	R4	Medium	Lower	The violation posed a minimal risk to the reliability of the bulk power system (BPS) because during the approximately three-month period, Buckeye Power had an Emergency Response (ERP) in place since April 2006. Although this ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation.	9/18/2007	8/21/2007	\$0	Self-report	Buckeye Power documented its specific FBI contact and applicable reporting procedure on September 21, 2007.	9/21/07	9/27/07	Neither Adm'd nor Denied
ERC	East Mississippi Electric Power Association (EMEPA)	NCR01206	ERC020100020	EMEPA had a violation of CIP-001-1, R1 because it did not have sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events provided to its operations personnel for the entire enforceable period.	CIP-001-1	R1	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. EMEPA had an ERP in place since April 2006. Although this ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation. 2. EMEPA does not own or operate any BPS facilities. 3. The violation duration was limited, because EMEPA mitigated the violation by September 28, 2007, and 4. EMEPA's peak load is approximately 200 MW.	9/18/2007	9/28/2007	\$4,000 (Settlement of ERC020100020, ERC020100021, and ERC020100022)	Audit	EMEPA developed a Sabotage Reporting Procedure with the required elements and provided to its operations personnel on September 28, 2007.	9/28/07	9/17/10	Neither Adm'd nor Denied
ERC	East Mississippi Electric Power Association (EMEPA)	NCR01206	ERC020100021	EMEPA had a violation of CIP-001-1, R1 because it did not have sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events provided to its operations personnel for the entire enforceable period.	CIP-001-1	R1	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. EMEPA had an ERP in place since April 2006. Although this ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation. 2. EMEPA does not own or operate any BPS facilities. 3. The violation duration was limited, because EMEPA mitigated the violation by September 28, 2007, and 4. EMEPA's peak load is approximately 200 MW.	9/18/2007	9/28/2007	\$4,000 (Settlement of ERC020100020, ERC020100021, and ERC020100022)	Audit	EMEPA developed a Sabotage Reporting Procedure with the required elements and provided to its operations personnel on September 28, 2007.	9/28/07	9/17/10	Neither Adm'd nor Denied
ERC	East Mississippi Electric Power Association (EMEPA)	NCR01206	ERC020100022	EMEPA had a violation of CIP-001-1, R3 because it did not have sabotage response guidelines, including personnel to contact, for reporting disturbances due to sabotage events provided to its operations personnel for the entire enforceable period.	CIP-001-1	R3	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. EMEPA had an ERP in place since April 2006. Although this ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation. 2. EMEPA does not own or operate any BPS facilities. 3. The violation duration was limited, because EMEPA mitigated the violation by September 28, 2007, and 4. EMEPA's peak load is approximately 200 MW.	9/18/2007	9/28/2007	\$4,000 (Settlement of ERC020100020, ERC020100021, and ERC020100022)	Audit	EMEPA developed a Sabotage Reporting Procedure with the required elements and provided to its operations personnel on September 28, 2007.	9/28/07	9/17/10	Neither Adm'd nor Denied
ERC	French Broad Electric Membership Corporation (French Broad)	NCR01244	ERC020100046	NERC staff found French Broad to be in violation of CIP-001-1, R1 because it failed 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, including at that stage in the process operating personnel are to be made aware of the event.	CIP-001-1	R1	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the BPS because: 1. The violation involves French Broad's registration as an LSE and French Broad has no generation or transmission BPS assets. As a RUS utility, French Broad had a RUS approved ERP in place. Although the ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation.	9/19/2007	9/11/2010	\$1,000 (Settlement of ERC020100046, ERC020100048, ERC020100049, and ERC020100052)	Audit	To correct the violation of CIP-001-1, R1, R2, R3 and R4, French Broad established and revised its procedures to meet the requirements of CIP-001, R1, R2, R3, and R4. Additionally, on November 1, 2009, French Broad hired a full time employee who, in addition to other responsibilities, is administering its CIP-001 procedures, along with training and posting of this procedure, was provided to all French Broad employees and conveyed information needed to identify and report suspected sabotage events thereby protecting the BPS and to prevent a recurrence of these violations.	12/17/2010 (one mitigation plan addressed the violation of R1-4)	11/8/10	Adm'd
ERC	French Broad Electric Membership Corporation (French Broad)	NCR01244	ERC020100050	NERC staff found French Broad to be in violation of CIP-001-1, R2 because it failed to have procedures for the communication of information concerning sabotage events to appropriate parties in the interconnection.	CIP-001-1	R2	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. The violation involves French Broad's registration as an LSE and French Broad has no generation or transmission BPS assets. As a RUS utility, French Broad had a RUS approved ERP in place. Although the ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation.	9/19/2007	9/26/2008	\$1,000 (Settlement of ERC020100046, ERC020100048, ERC020100049, and ERC020100052)	Audit	To correct the violation of CIP-001-1, R1, R2, R3 and R4, French Broad established and revised its procedures to meet the requirements of CIP-001, R1, R2, R3, and R4. Additionally, on November 1, 2009, French Broad hired a full time employee who, in addition to other responsibilities, is administering its CIP-001 procedures, along with training and posting of this procedure, was provided to all French Broad employees and conveyed information needed to identify and report suspected sabotage events thereby protecting the BPS and to prevent a recurrence of these violations.	12/17/2010 (one mitigation plan addressed the violation of R1-4)	11/8/10	Adm'd
ERC	French Broad Electric Membership Corporation (French Broad)	NCR01244	ERC020100051	NERC staff found French Broad to be in violation of CIP-001-1, R3 because it failed to have procedures for the communication of information concerning sabotage events to appropriate parties in the interconnection.	CIP-001-1	R3	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. The violation involves French Broad's registration as an LSE and French Broad has no generation or transmission BPS assets. As a RUS utility, French Broad had a RUS approved ERP in place. Although the ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation.	9/19/2007	10/27/2010	\$1,000 (Settlement of ERC020100046, ERC020100048, ERC020100049, and ERC020100052)	Audit	To correct the violation of CIP-001-1, R1, R2, R3 and R4, French Broad has established and revised its procedures to meet the requirements of CIP-001, R1, R2, R3, and R4. Additionally, on November 1, 2009, French Broad hired a full time employee who, in addition to other responsibilities, is administering its CIP-001 procedures, along with training and posting of this procedure, was provided to all French Broad employees and conveyed information needed to identify and report suspected sabotage events thereby protecting the BPS and to prevent a recurrence of these violations.	10/27/2010 (one mitigation plan addressed the violation of R1-4)	11/8/10	Adm'd
ERC	French Broad Electric Membership Corporation (French Broad)	NCR01244	ERC020100052	NERC staff found French Broad to be in violation of CIP-001-1, R4 because it did not establish communications contacts, as applicable, with local FBI officials and develop reporting procedures as appropriate to its circumstances.	CIP-001-1	R4	Medium	Severe	ERC determined that the violation posed a minimal risk to the reliability of the bulk power system (BPS) because: 1. The violation involves French Broad's registration as an LSE and French Broad has no generation or transmission BPS assets. As a RUS utility, French Broad had a RUS approved ERP in place. Although the ERP did not meet the specific requirements of CIP-001-1, it would have provided guidance on how to respond during an emergency situation.	9/19/2007	9/26/2008	\$1,000 (Settlement of ERC020100046, ERC020100048, ERC020100049, and ERC020100052)	Audit	To correct the violation of CIP-001-1, R1, R2, R3 and R4, French Broad has established and revised its procedures to meet the requirements of CIP-001, R1, R2, R3, and R4. Additionally, on November 1, 2009, French Broad hired a full time employee who, in addition to other responsibilities, is administering its CIP-001 procedures, along with training and posting of this procedure, was provided to all French Broad employees and conveyed information needed to identify and report suspected sabotage events thereby protecting the BPS and to prevent a recurrence of these violations.	12/17/2010 (one mitigation plan addressed the violation of R1-4)	11/8/10	Adm'd
Texas RE	Champion Wind Farm, LLC	NCR10173	TRE020000074	In the course of a June 2009 Audit, no documented facility ratings methodology was provided for the period from registration through December 3, 2008.	FAC-009-1	R1	Lower	Severe	The violation posed a minimal risk to BPS reliability because the Facility Ratings established pursuant to FAC-009-1, R1 spanned the entire audited period and were developed using a methodology that included the required considerations and reflected the Facility Ratings Methodology dated December 4, 2008.	2/1/2008	12/3/2008	\$4,500 (Settlement of TRE020000074, TRE020000075, TRE020000076, TRE020000077, and TRE020000078)	Audit	E.ON had a Facility Ratings Methodology in place as of December 4, 2008. The methodology provided by E.ON dated December 4, 2008 addressed all of the requirements of the Reliability Standard.	12/4/2008	11/4/2010	Neither Adm'd nor Denied
Texas RE	Forest Creek Wind Farm, LLC	NCR04003	TRE020000075	In the course of a June 2009 Audit, no documented facility ratings methodology was provided for the period from registration through December 3, 2008.	FAC-009-1	R1	Lower	Severe	The violation posed a minimal risk to the reliability of the bulk power system (BPS) because the Facility Ratings established pursuant to FAC-009-1, R1 spanned the entire audited period and were developed using a methodology that included the required considerations and reflected the Facility Ratings Methodology dated December 4, 2008.	6/29/2007	12/3/2008	\$4,500 (Settlement of TRE020000074, TRE020000075, TRE020000076, TRE020000077, and TRE020000078)	Audit	E.ON had a Facility Ratings Methodology in place as of December 4, 2008. The methodology provided by E.ON dated December 4, 2008 addressed all of the requirements of the Reliability Standard.	12/4/2008	11/4/2010	Neither Adm'd nor Denied
Texas RE	LCRAN Panther Creek Wind Farm & S, LLC	NCR10249	TRE020000076	In the course of a June 2009 Audit, no documented facility ratings methodology was provided for the period from registration through December 3, 2008.	FAC-009-1	R1	Lower	Severe	The violation posed a minimal risk to the reliability of the bulk power system (BPS) because the Facility Ratings established pursuant to FAC-009-1, R1 spanned the entire audited period and were developed using a methodology that included the required considerations and reflected the Facility Ratings Methodology dated December 4, 2008.	9/25/2008	12/3/2008	\$4,500 (Settlement of TRE020000074, TRE020000075, TRE020000076, TRE020000077, and TRE020000078)	Audit	E.ON had a Facility Ratings Methodology in place as of December 4, 2008. The methodology provided by E.ON dated December 4, 2008 addressed all of the requirements of the Reliability Standard.	12/4/2008	11/4/2010	Neither Adm'd nor Denied
Texas RE	Hoscoe Wind Farm, LLC	NCR10174	TRE020000077	In the course of a June 2009 Audit, no documented facility ratings methodology was provided for the period from registration through December 3, 2008.	FAC-009-1	R1	Lower	Severe	The violation posed a minimal risk to the reliability of the bulk power system (BPS) because the Facility Ratings established pursuant to FAC-009-1, R1 spanned the entire audited period and were developed using a methodology that included the required considerations and reflected the Facility Ratings Methodology dated December 4, 2008.	2/29/2008	12/3/2008	\$4,500 (Settlement of TRE020000074, TRE020000075, TRE020000076, TRE020000077, and TRE020000078)	Audit	E.ON had a Facility Ratings Methodology in place as of December 4, 2008. The methodology provided by E.ON dated December 4, 2008 addressed all of the requirements of the Reliability Standard.	12/4/2008	11/4/2010	Neither Adm'd nor Denied
Texas RE	Sand Bluff Wind Farm, LLC	NCR04004	TRE020000078	In the course of a June 2009 Audit, no documented facility ratings methodology was provided for the period from registration through December 3, 2008.	FAC-009-1	R1	Lower	Severe	The violation posed a minimal risk to the reliability of the bulk power system (BPS) because the Facility Ratings established pursuant to FAC-009-1, R1 spanned the entire audited period and were developed using a methodology that included the required considerations and reflected the Facility Ratings Methodology dated December 4, 2008.	11/1/2008	12/3/2008	\$4,500 (Settlement of TRE020000074, TRE020000075, TRE020000076, TRE020000077, and TRE020000078)	Audit	E.ON had a Facility Ratings Methodology in place as of December 4, 2008. The methodology provided by E.ON dated December 4, 2008 addressed all of the requirements of the Reliability Standard.	12/4/2008	11/4/2010	Neither Adm'd nor Denied
Texas RE	LCRA Transmission Services Corporation	NCR04081	TRE020100010	One LPLS relay was tested outside the 60-month interval. LPLS relay on Gonzalez Panel 14 had been inductively tested when the LPLS relay on Gonzalez Panel 4 should have been tested instead. Panel 4 was tested on June 24, 2004, was scheduled to be tested on October 7, 2008, but was due for testing on June 24, 2009. The test was performed on June 14, 2010.	PRC-009-0	R2	Medium	Lower	The violation posed a minimal risk to the reliability of the bulk power system (BPS). The peak demand on the affected relay is approximately 1.8 MW. Further, LCRA TSC's present load under LPLS would have been 11.1% had the relay failed, leaving them well above the ERCOT minimum requirement of 5%, in addition, when the subject relay was tested, it was found to be within tolerance.	6/24/2009	6/14/2010	\$0	Self-report	Immediately upon recognizing that the subject relay required testing, LCRA TSC conducted testing of the relay on June 14, 2010 to verify proper operation. LCRA TSC updated its LCRA Substation Operators LPLS Maintenance and Testing procedures. The first step in the updated procedure reads "Verify relay ID and equipment record corresponds to relay under test. If information does not correspond, contact the applicable LCRA Reliability Coordinator or their supervisor."	7/15/2010	11/15/2010	Adm'd
Texas RE	Tex-La Electric Cooperative of Texas, Inc.	NCR03142	TRE020000084	Tex-La Electric did not have a complete program identifying the LPLS equipment. It also did not have a schedule for the testing nor maintenance of the relay. A spare schedule from another Tex-La Electric's procedure, but it did not include any equipment identification or schedule dates. Texas RE conducted its audit of Tex-La Electric jointly with SPP because Tex-La Electric's equipment spanned both regions. SPP issued a non-compliance violation of PRC-009-0 during the audit. Finally, Tex-La Electric is a member of the East Texas Electric Cooperative, which had a prior violation of PRC-009-0. Tex-La Electric's membership in the cooperative was not sufficient to serve as an aggravating factor in determining the penalty amount in the settlement.	PRC-009-0	R1	Medium	Severe	This violation posed a minimal risk to the reliability of the bulk power system (BPS) because there were test reports provided that demonstrated that the relay had been tested in 2009 even though the LPLS equipment identification and schedules were not documented. Tex-La Electric was subject to a non-compliance violation by Texas RE, where it provided a maintenance and testing schedule. According to the entity, this was mistakenly removed from its procedure in between the spot check and the audit.	11/20/2007	4/30/2009	\$1,000	Audit	Tex-La notified its Proxy, Guidelines, and Procedures to incorporate a reference to Tex-La TSC LPLS.doc (Formerly a blank form in BTEC's previous procedure). This document includes the information referred to the Standard.	5/23/2010	6/25/2010	Neither Adm'd nor Denied

20110201-5148 FERC PDF (Unofficial) 1/31/2011 8:15:48 PM

Document Content(s)

FinalFiled_ACP Jan 31 2011.PDF.....	1-12
Public_Final_Filed_A-2.XLS.....	13-14
Public_FinalFiled_A-1.XLS.....	15-15