



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 Penalty<sup>1</sup> (Administrative Citation NOP) in Attachment A regarding 19 Registered Entities<sup>2</sup> listed therein,<sup>3</sup> 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)).<sup>4</sup>

The Administrative Citation NOP resolves 41 violations<sup>5</sup> 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

---

<sup>1</sup> *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).

<sup>2</sup> Corresponding NERC Registry ID Numbers for each Registered Entity are identified in Attachment A.

<sup>3</sup> Attachment A consists of three excel spreadsheets.

<sup>4</sup> See 18 C.F.R. § 39.7(c)(2).

<sup>5</sup> 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.<sup>6</sup> 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 Mitigation<sup>7</sup>**

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.

---

<sup>6</sup> 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).

<sup>7</sup> 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 Imposed<sup>8</sup>**

### **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,<sup>9</sup> 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.

---

<sup>8</sup> See 18 C.F.R § 39.7(d)(4).

<sup>9</sup> *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 Publication<sup>10</sup>**

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>	

<sup>10</sup> 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](mailto: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](mailto:se.patrick@midwestreliability.org)

**FOR NPCC:**

Walter Cintron\*  
Manager, Compliance Enforcement  
Northeast Power Coordinating Council, Inc.  
1040 Avenue of the Americas – 10<sup>th</sup> Floor  
New York, New York 10018-3703  
(212) 840-1070  
(212) 302-2782 – facsimile  
[wcintron@npcc.org](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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](mailto: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. (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	Adm'd or Neither Adm'd nor Denied
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 Adm'd nor Denied
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 Adm'd nor Denied
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 Adm'd nor Denied
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 noticed 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 performance scan on the relevant server to ensure the change did not introduce a new port or service. Network administrators would have analyzed 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	Adm'd



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