NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

December 22, 2010

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

Re: NERC Deficiency Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP11-__-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Deficiency Notice of Penalty (Deficiency NOP) regarding Unidentified Registered Entity (URE),[1] 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)). Violations[2] addressed within a Deficiency NOP are administrative, minor or documentation in nature. In this case, the violation was minor because URE was only one day late in assessing its security patches and the patches were implemented on the same schedule as they would have been if they were assessed one day earlier.

The "Notice of Penalty Waiver and Settlement Agreement" (Settlement Agreement) dated December 6, 2010 between URE and SERC Reliability Corporation (SERC) resolves all outstanding issues arising from SERC's determination and findings of the enforceable violation of CIP-007-1 Requirement (R) 3.1. According to the Settlement Agreement, URE neither admits nor denies the violation, but has agreed to the assessed penalty of two thousand dollars ($2,000) in addition to other remedies and actions to mitigate the instant violation and facilitate future compliance under the terms and conditions of the Settlement Agreement.

[1] The Disposition Document addresses: (1) all relevant facts, in sufficient detail, to indicate the nature of the violation cited and its duration; (2) sufficient information on whether an entity did not perform the action required by the relevant Reliability Standard or failed to document that the action had been performed; (3) a linkage between specific facts and the penalty factors listed as relevant to the penalty determination; (4) specific information in a mitigation plan how a registered entity will comply with the requirements it has violated; and (5) specific information on how a Regional Entity verified that a registered entity timely completed a mitigation plan.

[2] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

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

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[3] the NERC BOTCC reviewed the findings and assessed penalty or sanction and approved the Settlement Agreement on October 12, 2010, including SERC's assessment of a two thousand dollar ($2,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30 day period following the filing of this Deficiency NOP with the Commission, or, if the Commission decides to review the penalty, upon final determination by the Commission.

Request for Confidential Treatment

Information in and certain attachments to the instant Notice of Penalty include privileged and 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. Specifically, this includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business and confidential information exempt from the mandatory public disclosure requirements of the Freedom of Information Act, 5 U.S.C. 552, and should be withheld from public disclosure.

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 attached documents are 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.

[3] *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*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

Attachments to be included as Part of this Notice of Penalty

The attachments to be included as part of this Deficiency NOP are the following documents:

a) Settlement Agreement by and between SERC and URE executed December 6, 2010, included as Attachment a;

    a. Disposition of Violation and Verification of Completion therein, included as Attachment A to the Settlement Agreement;

b) URE's Self-Report dated February 18, 2010, included as Attachment b;

c) URE's Mitigation Plan submitted February 18, 2010, included as Attachment c; and

d) URE's Certification of Mitigation Plan Completion dated July 30, 2010, included as Attachment d.

A Form of Notice Suitable for Publication[4]

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

[4] *See* 18 C.F.R. § 39.7(d)(6).

Notices and Communications

Notices and communications with respect to this filing may be addressed to the following:

Gerald W. Cauley President and Chief Executive Officer David N. Cook* Sr. 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 Kenneth B. Keels, Jr.* Director of Compliance Andrea Koch* Manager of 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	Rebecca J. Michael* Assistant General Counsel Davis Smith* Attorney North American Electric Reliability Corporation 1120 G Street, N.W. Suite 990 Washington, DC 20005-3801 (202) 393-3998 (202) 393-3955 – facsimile rebecca.michael@nerc.net davis.smith@nerc.net 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 Jacqueline E. Carmody* Legal Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org jcarmody@serc1.org *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.

Conclusion

Accordingly, NERC respectfully requests that the Commission accept this Deficiency NOP as compliant with its rules, regulations and orders.

Respectfully submitted,

Gerald W. Cauley
President and Chief Executive Officer
David N. Cook
Sr. 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

/s/ *Rebecca J. Michael*
Rebecca J. Michael
Assistant General Counsel
Davis Smith
Attorney
North American Electric Reliability Corporation
1120 G Street, N.W.
Suite 990
Washington, DC 20005-3801
(202) 393-3998
(202) 393-3955 – facsimile
rebecca.michael@nerc.net
davis.smith@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Disposition of Violation and Verification of Completion therein

Attachment A

DISPOSITION OF VIOLATION[1]
Dated December 6, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.	NOC#
SERC201000493	**10-067**	**NOC-663**

REGISTERED ENTITY
Unidentified Registered Entity ("URE")

NERC REGISTRY ID
NCRXXXXX

REGIONAL ENTITY
SERC Reliability Corporation ("SERC")

I. VIOLATION INFORMATION

RELIABILITY STANDARD	REQUIREMENT(S)	SUB-REQUIREMENT(S)	VRF(S)	VSL(S)
CIP-007-1	**3**	**3.1**	**Lower**	**Lower**

PURPOSE OF THE RELIABILITY STANDARD AND TEXT OF RELIABILITY STANDARD AND REQUIREMENT(S)/SUB-REQUIREMENT(S)

The purpose statement of CIP-007-1 provides in pertinent part: "Standard CIP-007-1 requires Responsible Entities[2] to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009…."

CIP-007-1 R3 provides:

R3. Security Patch Management —The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

[1] For purposes of this document and attachments hereto, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.
[2] Within the text of the Reliability Standard, "Responsible Entity" shall mean: Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC and Regional Reliability Organizations.

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

VIOLATION DESCRIPTION

On February 18, 2010, URE submitted a Self-Report to SERC for a violation of CIP-007-1, R3.1 upon discovery that its security patch identification application had not identified two security patches; thus, URE had not performed the required assessment of those two security patches within 30 days of availability of such patches.

SERC staff reviewed URE's self-report and the information provided by URE regarding its failure to assess the two security patches for its cyber security software in a timely manner. Pursuant to CIP-007-1, R3.1 and the patch program ("program"), URE is required to document the assessment of security patches and security upgrades for applicability within thirty (30) days of the availability of the patches or upgrades.

To comply with this program, URE utilizes a patching application widely used in the industry from a leading software vendor that, among other things, automatically: (1) interfaces with the operating system vendor; (2) scans all of the patches offered for the installed operating system; (3) and places all of those patches in a repository. The patching application then analyzes the software on each Critical Cyber Asset ("CCA") server and compares it with the repository to determine if any security patches are applicable. The report that results from the analysis reflects all applicable security patches and those security patches are assessed by a URE subject matter expert ("SME"). In accordance with the program, if the URE SME determines that a security patch is to be applied, URE's transmission business unit and the IT business unit affiliated with URE determine an implementation date and the security patch is scheduled for implementation.

On January 4, 2010, the patching application for the CCA servers ran as expected, obtained the security patches released on that date, and placed those security patches in the repository. The January 4, 2010 patching application report ("January 4th Report") did not match all of the security patches to each affected server and reflect those security patches in the report. In accordance with CIP-007-1, R3.1 and the program, an assessment of the security patches from the January 4, 2010 patching application was due February 3, 2010.

On February 2, 2010, the IT assessment of the January 4th Report revealed an unusually small amount of patches associated with the patching application of the same date.

On February 3 and 4, 2010, IT conducted a review to ascertain external patch sources for potential applicable patches and validated the patching process. IT confirmed that the January 4th Report did not identify two applicable security patches for the operating system on the CCA servers.

On February 4, 2010, IT immediately contacted technical support for the vendor of URE's patching application who stated that a component in the patching application needed to be modified to permit the application to identify all of the appropriate security patches. The patching application was modified that same day and then the automatic assessment process performed as intended.

Also on February 4, 2010, IT implemented a manual process to identify the appropriate patches and facilitate its review. The two patches were assessed on February 4, 2010 and URE determined that the two patches were applicable to all hosts running the affected operating system. The two patches were scheduled to be implemented in accordance with URE's regularly scheduled system maintenance cycle, which was conducted beginning March 12, 2010 and completed on April 13, 2010.

The two patches affected a total of nine URE systems. Three of the nine systems are CCAs and the remaining six are Cyber Assets within the Electronic Security Perimeter ("ESP"). The nine assets running the affected operating system represent 7.5 % of the total number of assets (CCAs and Cyber Assets) within the ESP.

SERC concluded that the facts and evidence supported a finding that URE violated CIP-007-1 R3.1 because URE conducted the patch assessment for two security patches 31 days after the date the patches were available, which was 1 day beyond the Standard's requirement of assessing patches for applicability within 30 calendar days of the date the patches became available.

RELIABILITY IMPACT STATEMENT- POTENTIAL AND ACTUAL

SERC staff finds that the violation did not pose a serious or substantial risk to the reliability of the bulk power system ("BPS") because:

1. **URE employed a twice monthly patch assessment process, including a review and comparison of each patch application report, instead of the 30-day interval required by the Standard. Although inconsistent with the timelines in the Standard, this practice did enhance the ability of URE to identify missed patch assessments and reduces the timeframe in which a missed patch assessment would persist; and**
2. **the patches in question were subsequently assessed, and the delay in assessment did not affect the time period when the patches were scheduled to be implemented. All patches have since been installed on the affected systems in a timely fashion. The patches were installed within the same regularly scheduled maintenance cycle that they would have fallen under if they were assessed during the 30-day window as prescribed by the Standard.**

IS THERE A SETTLEMENT AGREEMENT YES ☒ NO ☐

Attachment A

WITH RESPECT TO THE VIOLATION(S), REGISTERED ENTITY

NEITHER ADMITS NOR DENIES IT (SETTLEMENT ONLY)	YES	☒
ADMITS TO IT	YES	☐
DOES NOT CONTEST IT (INCLUDING WITHIN 30 DAYS)	YES	☐

WITH RESPECT TO THE ASSESSED PENALTY OR SANCTION, REGISTERED ENTITY

ACCEPTS IT/ DOES NOT CONTEST IT	YES	☒

III. DISCOVERY INFORMATION

METHOD OF DISCOVERY

SELF-REPORT	☒
SELF-CERTIFICATION	☐
COMPLIANCE AUDIT	☐
COMPLIANCE VIOLATION INVESTIGATION	☐
SPOT CHECK	☐
COMPLAINT	☐
PERIODIC DATA SUBMITTAL	☐
EXCEPTION REPORTING	☐

DURATION DATE(S) **2/3/10 through 2/4/10 when a URE SME assessed the missed patches and scheduled them for implementation**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **2/18/10**

IS THE VIOLATION STILL OCCURRING	YES	☐	NO	☒
IF YES, EXPLAIN				

REMEDIAL ACTION DIRECTIVE ISSUED	YES	☐	NO	☒
PRE TO POST JUNE 18, 2007 VIOLATION	YES	☐	NO	☒

IV. MITIGATION INFORMATION

FOR FINAL ACCEPTED MITIGATION PLAN:

MITIGATION PLAN NO.	**MIT-10-2704**
DATE SUBMITTED TO REGIONAL ENTITY	**2/18/10**[3]
DATE ACCEPTED BY REGIONAL ENTITY	**7/26/10**
DATE APPROVED BY NERC	**8/19/10**
DATE PROVIDED TO FERC	**8/20/10**

[3] The Mitigation Plan was signed on February 16, 2010.

Attachment A

IDENTIFY AND EXPLAIN ALL PRIOR VERSIONS THAT WERE ACCEPTED OR REJECTED, IF APPLICABLE

MITIGATION PLAN COMPLETED YES ☒ NO ☐

EXPECTED COMPLETION DATE	**4/17/10**
EXTENSIONS GRANTED	**N/A**
ACTUAL COMPLETION DATE	**4/17/10**
DATE OF CERTIFICATION LETTER	**7/30/10**
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	**4/17/10**
DATE OF VERIFICATION	**8/11/10**[4]
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	**4/17/10**

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

To correct the violation of CIP-007-1 R3.1, the IT used an electronic vendor solution to identify a list of patches applicable to the affected asset, and the URE patch management application is configured to analyze an asset for missing patches based on the configuration of the Critical Assets/CCAs within the ESP resulting in a report to confirm which patches are required. Additionally, IT personnel performed a manual process to confirm the automated system has retrieved and matched the appropriate security patches.

LIST OF EVIDENCE REVIEWED BY REGIONAL ENTITY TO EVALUATE COMPLETION OF MITIGATION PLAN (FOR CASES IN WHICH MITIGATION IS NOT YET COMPLETED, LIST EVIDENCE REVIEWED FOR COMPLETED MILESTONES)

URE submitted the following as evidence of completion of its mitigation plan:

1. **A screenshot detailing URE's update job, dated May 3, 2010 which demonstrated the process that had been used for patch assessment and the results of the application of that process;**
2. **an Excel spreadsheet showing URE's patch analysis, dated January 14, 2010 which demonstrated the process that had been used for patch assessment and the results of the application of that process;**
3. **an Excel spreadsheet which is URE's NERC patch assessment document for Unix and Linux Server Patch Management, dated December 9, 2009 and posted to a SharePoint repository on February 17, 2010 and that demonstrated the process that**

[4] This Disposition Document serves as SERC's Verification of Mitigation Plan Completion.

had been used for patch assessment and the results of the application of that process;

4. **a before screenshot showing the script for the process that resulted in the violation, dated May 1, 2010;**
5. **an after screenshot showing the script for the process after editing that corrected the cause of the violation, dated May 1, 2010;**
6. **a support ticket, dated February 4, 2010, reporting the concern to the patch management system vendor and requesting resolution of the identified issue;**
7. **a word document, dated March 12, 2010 which showed that the implementation process for patching had been started;**
8. **a document, dated March 12, 2010 which demonstrated completion of a tracking item to correct this issue; and**
9. **a report prepared by the URE SME, dated February 18, 2010 documenting a determination of the impact of the two missing patches on the reliability of the Bulk Electric System (BES).**

V. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **$2,000** FOR **ONE** VIOLATION OF RELIABILITY STANDARDS.

(1) REGISTERED ENTITY'S COMPLIANCE HISTORY

PREVIOUSLY FILED VIOLATIONS OF ANY OF THE INSTANT RELIABILITY STANDARD(S) OR REQUIREMENT(S) THEREUNDER
YES ☐ NO ☐

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

PREVIOUSLY FILED VIOLATIONS OF OTHER RELIABILITY STANDARD(S) OR REQUIREMENTS THEREUNDER
YES ☐ NO ☐

LIST VIOLATIONS AND STATUS

ADDITIONAL COMMENTS

(2) THE DEGREE AND QUALITY OF COOPERATION BY THE REGISTERED ENTITY (IF THE RESPONSE TO FULL COOPERATION IS "NO," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

FULL COOPERATION YES ☒ NO ☐
IF NO, EXPLAIN

(3) THE PRESENCE AND QUALITY OF THE REGISTERED ENTITY'S COMPLIANCE PROGRAM

IS THERE A DOCUMENTED COMPLIANCE PROGRAM
YES ☒ NO ☐ UNDETERMINED ☐
EXPLAIN

URE has a documented Internal Compliance Program ("ICP") which SERC considered a mitigating factor in determining the penalty.

EXPLAIN SENIOR MANAGEMENT'S ROLE AND INVOLVEMENT WITH RESPECT TO THE REGISTERED ENTITY'S COMPLIANCE PROGRAM, INCLUDING WHETHER SENIOR MANAGEMENT TAKES ACTIONS THAT SUPPORT THE COMPLIANCE PROGRAM, SUCH AS TRAINING, COMPLIANCE AS A FACTOR IN EMPLOYEE EVALUATIONS, OR OTHERWISE.

(4) ANY ATTEMPT BY THE REGISTERED ENTITY TO CONCEAL THE VIOLATION(S) OR INFORMATION NEEDED TO REVIEW, EVALUATE OR INVESTIGATE THE VIOLATION.

YES ☐ NO ☒
IF YES, EXPLAIN

(5) ANY EVIDENCE THE VIOLATION(S) WERE INTENTIONAL (IF THE RESPONSE IS "YES," THE ABBREVIATED NOP FORM MAY NOT BE USED.)

YES ☐ NO ☒
IF YES, EXPLAIN

(6) ANY OTHER MITIGATING FACTORS FOR CONSIDERATION

YES ☒ NO ☐
IF YES, EXPLAIN

The potential violation was discovered through a self-initiated independent verification. URE proactively: (i) investigated the unusually small amount of patches prior to the end of the 30-day time frame required in CIP-007 R3.1; (ii) immediately initiated a manual independent verification of the automated patching process; and (iii) assessed the patches within 24 hours of confirming the patches were omitted.

(7) ANY OTHER AGGRAVATING FACTORS FOR CONSIDERATION

YES ☐ NO ☒
IF YES, EXPLAIN

(8) ANY OTHER EXTENUATING CIRCUMSTANCES

YES ☐ NO ☒
IF YES, EXPLAIN

EXHIBITS:

SOURCE DOCUMENT
Self-Report dated February 18, 2010

MITIGATION PLAN
Mitigation Plan submitted February 18, 2010

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion dated July 30, 2010

Attachment A

OTHER RELEVANT INFORMATION:

NOTICE OF ALLEGED VIOLATION AND PROPOSED PENALTY OR SANCTION ISSUED
DATE: OR N/A ☒

SETTLEMENT DISCUSSIONS COMMENCED
DATE: **3/3/10** OR N/A ☐

NOTICE OF CONFIRMED VIOLATION ISSUED
DATE: OR N/A ☒

SUPPLEMENTAL RECORD INFORMATION
DATE(S) OR N/A ☒

REGISTERED ENTITY RESPONSE CONTESTED
FINDINGS ☐ PENALTY ☐ BOTH ☐ NO CONTEST ☒

HEARING REQUESTED
YES ☐ NO ☒
DATE
OUTCOME
APPEAL REQUESTED