



NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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)). Violations² addressed within a Deficiency NOP are administrative, minor or documentation in nature. In this case, URE did not maintain its list of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and corresponding access rights information, in one location and had not been maintaining a historical record of changes to the list.

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-004-1 Requirement (R) 4. According to the Settlement Agreement, URE neither admits nor denies the violation, but has agreed to the assessed penalty of zero dollars (\$0) 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.

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 zero dollar (\$) 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;
 1. Disposition Document and Verification of Mitigation Plan Completion contained therein, included as Attachment A to the Settlement Agreement;
- b) Spot Check Screening Worksheet, included as Attachment b;
- c) URE's Mitigation Plan MIT-09-2558 dated December 2, 2009, included as Attachment c; and
- d) URE's Certification of Mitigation Plan Completion dated December 30, 2009, included as Attachment d.

A Form of Notice Suitable for Publication⁴

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:

<p>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</p> <p>Kenneth B. Keels, Jr.* Director of Compliance Andrea Koch* Manager of Compliance Enforcement and Mitigation SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8214 (704) 357-7914 – facsimile kkeels@serc1.org akoch@serc1.org</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.</p>	<p>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</p> <p>R. Scott Henry* President and CEO SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8202 (704) 357-7914 – facsimile shenry@serc1.org</p> <p>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</p>
---	---

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

**Disposition Document and Verification of
Mitigation Plan Completion contained therein**

DISPOSITION OF VIOLATION¹
Dated December 6, 2010

NERC TRACKING NO.	REGIONAL ENTITY TRACKING NO.	NOC#
SERC200900392	09-153	NOC-620

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-004-1	4	4.1	Lower	High²

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

The purpose statement of CIP-004-1 provides in pertinent part: “Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009....”

CIP-004-1 R4 provides:

R4. Access — The Responsible Entity^[3] shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to

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 The total number of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets (CCAs) on URE’s access list is fifty-eight; eight vendors (14%) were missing from the access list provided during the Spot-Check. In addition, URE did not update its access list(s) within seven calendar days of a change of personnel with such access to CCAs. Also, URE did not update any change in the access rights of such personnel.

³ Within the text of Standard CIP-004, “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.

Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

(Footnote added.)

VIOLATION DESCRIPTION

SERC sent URE a notice of a SERC CIP spot-check audit of URE (Spot Check). The SERC spot-check team conducted its Spot Check of URE to determine compliance with the NERC Reliability Standards.⁴

Prior to July 28, 2009, URE used a Microsoft Access database (Access database) to maintain its list of employees, contractors and service personnel with authorized cyber and authorized unescorted physical access to its Critical Cyber Assets (CCAs). URE did not log dates and times of modifications made to individual records in the database; thus the Access database retained only the most current date of modifications or additions to the list for each individual record. On July 28, 2009, URE implemented a revised procedure, which required maintaining its lists of employees, contractors and service vendors with authorized access to CCAs in spreadsheets that tracked file revisions and the date of each modification rather than using the Access database. During this process improvement, URE failed to migrate the dates upon which access was first granted to individuals, the dates the access list was updated, and any authorized vendor names or information from the Access database to the spreadsheet.

During the Spot Check, SERC identified two incidents in which URE failed to properly maintain its lists of employees, contractors and service vendors with authorized cyber or authorized unescorted physical access to CCAs, and failed to include the individuals' specific electronic and physical access rights to CCAs on such lists. First, URE provided the Spot Check team with its current CCA access spreadsheet and stated it was accurate. According to URE, it had not removed

⁴ URE is a Responsible Entity that was required to self-certify compliance to NERC's Urgent Action Cyber Security Standard 1200 (UA 1200) and is therefore a "Table 1 Entity" under the Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1. As such, URE was required to be "Compliant" with CIP-004-1 R4 as of July 1, 2008 and "Auditably Compliant" as of July 1, 2009.

access for any personnel from the spreadsheet and only one individual had been granted authorized unescorted physical access or authorized cyber access to URE's CCAs since the date CIP-004-1 R4 became mandatory and enforceable. The Spot Check team reviewed the spreadsheet and identified that on March 25, 2009, a URE employee who was listed in the spreadsheet URE provided, was granted unescorted physical access to URE's CCAs. URE could not produce evidence that its spreadsheet had been updated to include this employee within seven (7) calendar days of the unescorted physical access but the Spot Check team did validate that the spreadsheet was accurate for the balance of URE employees included on the spreadsheet. During the Spot Check, URE produced additional evidence regarding the URE employee's access to the CCAs in the form of a memo dated April 9, 2009, which showed that the employee had been granted authorized access, but the memo was dated more than seven days from the date access was granted.

Second, in addition to the most current CCA access spreadsheet, URE presented a memo listing vendor personnel with authorized cyber access dated November 2, 2009, in response to a query from the Spot Check team about URE's performance of background checks. URE stated that it had an Energy Management System vendor who serviced its equipment and had access to CCAs prior to November 2, 2009. URE's access spreadsheet did not include the names of vendor personnel or further information about any vendor personnel (including the Energy Management System vendor), but the November 2, 2009 memo did list the names of such vendors who had been granted authorized access to URE's CCAs. Nevertheless, the memo was deficient as evidence of compliance with CIP-004-1 R4 because it did not include the vendors' specific electronic and physical access rights to CCAs and it did not authorize access before November 2, 2009.

Upon receipt of the findings from the Spot Check, SERC Compliance Enforcement staff commenced its detailed assessment. During the assessment, SERC Compliance Enforcement staff interviewed the Spot Check team, URE CIP subject matter experts and compliance personnel, and requested additional information from URE to assist in its assessment. On February 9, 2010, after discussions with SERC Compliance Enforcement staff, URE provided the Access database used to track authorized personnel access prior to the July 28, 2009 change to its spreadsheet; however, URE's subject matter expert did not present this evidence during the Spot Check, due to an oversight. Upon review of the Access database, SERC Compliance Enforcement staff noted that the employee was in fact included in the Access database as having authorized unescorted access when CCAs were accessed on March 25, 2009, and did not receive their access key to the CCAs until March 31, 2009, after they had been added to the list maintained in the Access database. SERC Compliance Enforcement staff also noted that the vendors identified by the Spot Check team as missing from the spreadsheet were in fact included in the Access database with authorized access prior to URE's transition to the new spreadsheet on July 28, 2009.

PERIODIC DATA SUBMITTAL
 EXCEPTION REPORTING

DURATION DATE(S) **4/1/2009 (7 days after employee was granted access to the CCAs) through 11/14/09 (Mitigation Plan completion)**

DATE DISCOVERED BY OR REPORTED TO REGIONAL ENTITY **11/11/09**

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-09-2558
DATE SUBMITTED TO REGIONAL ENTITY	12/2/09
DATE ACCEPTED BY REGIONAL ENTITY	5/5/10
DATE APPROVED BY NERC	6/25/10
DATE PROVIDED TO FERC	6/28/10

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

N/A

MITIGATION PLAN COMPLETED YES NO

EXPECTED COMPLETION DATE	Submitted as complete
EXTENSIONS GRANTED	N/A
ACTUAL COMPLETION DATE	11/14/09

DATE OF CERTIFICATION LETTER	12/30/09
CERTIFIED COMPLETE BY REGISTERED ENTITY AS OF	11/14/09

DATE OF VERIFICATION	3/18/10⁵
VERIFIED COMPLETE BY REGIONAL ENTITY AS OF	11/14/09

ACTIONS TAKEN TO MITIGATE THE ISSUE AND PREVENT RECURRENCE

⁵ This Disposition Document serves as SERC's Verification of Mitigation Plan Completion.

To correct the violation of CIP-004-1 R4, URE was required to and has completed the following actions detailed in its Mitigation Plan:

1. Immediately following identification of the violation, URE thoroughly reviewed its current procedure and methods for updating its list of personnel with authorized cyber and authorized unescorted physical access to CCAs and acknowledged that this particular violation is strictly a documentation oversight; and
2. URE added the list of contractors that had been omitted from the previous method URE used for updating and maintaining its list of personnel with authorized cyber and authorized unescorted physical access to CCAs.

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 its completion of its Mitigation Plan:

1. URE's database dated February 9, 2010, which showed a complete list of all personnel, contractors and service vendors who have access to CCAs; and
2. a pdf of URE's electronic access list dated November 12, 2009, which showed an accurate list of all personnel who have access to CCAs.

V. PENALTY INFORMATION

TOTAL ASSESSED PENALTY OR SANCTION OF **ZERO DOLLARS (\$0)** 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

SERC considered the existence of URE's internal compliance plan as 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

(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
Spot Check Screening Worksheet

MITIGATION PLAN
Mitigation Plan, MIT-09-2558, dated December 2, 2009

CERTIFICATION BY REGISTERED ENTITY
Certification of Mitigation Plan Completion dated December 30, 2009

VERIFICATION BY REGIONAL ENTITY
This Disposition Document serves as SERC's Verification of Mitigation Plan Completion

OTHER RELEVANT INFORMATION:

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

SETTLEMENT DISCUSSIONS COMMENCED

DATE: **12/4/09** 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