

May 30, 2012

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

**Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity,
FERC Docket No. NP12-_-000**

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty¹ regarding Unidentified Registered Entity (URE) NERC Registry ID# NCRXXXXX, 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)).²

URE submitted a Self-Report addressing a violation³ of CIP-005-1 R2. Based on the Self-Report and additional information from URE, the Western Electricity Coordinating Council (WECC) determined URE failed to implement and maintain its procedure for securing dial-up access to its Electronic Security Perimeter (ESP), in violation of this Standard.

URE submitted a Self-Report stating that it had discovered that an employee had gained unescorted access into a Physical Security Perimeter (PSP) on three occasions. Based on the record, WECC determined URE failed to ensure appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls, in

¹ *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). See also 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). See 18 C.F.R § 39.7(c)(2).

² See 18 C.F.R § 39.7(c)(2).

³ 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 Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 2

violation of CIP-006-3c R1.4. In addition, WECC determined URE failed to ensure that a visitor was escorted and signed-in as per URE's visitor escort procedure, in violation of CIP-006-3c R1.6.

This Notice of Penalty is being filed with the Commission because, based on information from WECC, URE accepted the violations of CIP-005-1 R2 and CIP-006-3c R1 and the proposed one hundred sixty-two thousand two hundred dollar (\$162,200) penalty to be assessed to URE. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201102522 and WECC201102887 are Confirmed Violations, as that term is defined in the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) issued on October 12, 2011, by WECC. The details of the findings and basis for the penalty are set forth in the NOCV and herein. This Notice of Penalty filing contains the basis for approval of the NOCV by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2011), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty (\$)
WECC	Unidentified Registered Entity	NOC-1019	WECC201102522	CIP-005-1	R2	Medium ⁴	\$162,200
			WECC201102887	CIP-006-3c	R1	Medium ⁵	

CIP-005-1 R2 (WECC201102522)

The purpose of Reliability Standard CIP-005-1 provides: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as

⁴ CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" Violation Risk Factor (VRF); CIP-005-1 R2.5 and its subrequirements, and R2.6 each have a "Lower" VRF.

⁵ CIP-006-3c R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6, R1.6.1 and R1.6.2 each have a "Medium" VRF; CIP-006-3c R1.7 and R1.8 each have a "Lower" VRF. In the context of this case, WECC determined the violation applied to both R1.4 and R1.6.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 3

well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.”

CIP-005-1 R2 provides:

R2. Electronic Access Controls — The Responsible Entity^[6] shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

⁶ Within the text of Standard CIP-002 - 009, “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.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 4

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R2 has a “Medium” Violation Risk Factor (VRF) and a “Severe” Violation Severity Level (VSL).

URE submitted a Self-Report, stating that it failed to maintain a procedure for securing dial-up access to the ESP as required by CIP-005-1 R2. WECC reviewed URE’s Self-Report and conducted a phone interview, during which, URE confirmed an engineer attempted to remotely access a relay (a Critical Asset within an ESP) to extract the relay event report in response to a transmission line fault. Since URE’s standard method for accessing ESPs via a centralized access system did not work, the engineer attempted to use the old method of dialing a modem number for a communication processor to the relay. The dial-up attempt was successful, and the required task was completed.

URE’s policy prohibits the use of dial-up connections to Critical Assets and Critical Cyber Assets (CCAs). The legacy modem line used to connect to the equipment at the substation should have been disabled as part of a project that was completed years earlier, but a review of the work orders revealed inconsistencies on the completion statements. The engineer’s supervisor went to the substation and unplugged the modem connection.

Based on the record, WECC determined URE failed to implement and maintain its procedure for securing dial-up access to the ESP, in violation of CIP-005-1 R2.

WECC determined the duration of the violation to be from the date the Standard became enforceable, to when URE completed its Mitigation Plan.

WECC determined that this violation did not pose a serious or substantial risk and posed a moderate risk to the reliability of the bulk power system (BPS). Although the device used to connect to the relay allowed access to an additional number of relays, all of which are Critical Assets, and a failure to document and implement mechanisms for control of electronic access to the ESP could potentially

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 5

expose the CCAs within the ESP to security attacks, there were security measures in place to prevent access to the CCAs. The devices used to remotely connect to relays require a username and password and are located within an ESP and PSP, thus reducing the risk to the BPS. In addition, in this case, the engineer who accessed the relay had current CIP training and a current personnel risk assessment (PRA).

Status of Mitigation Plan⁷

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC on May 27, 2011 with a proposed completion date of November 1, 2011. The Mitigation Plan was accepted by WECC on June 28, 2011 and approved by NERC on July 25, 2011. The Mitigation Plan for this violation is designated as MIT-11-3877 and was submitted as non-public information to FERC on July 27, 2011 in accordance with FERC orders.

According to the Mitigation Plan, URE:

1. Established a project/initiative to physically visit every ESP that had modem connections prior to the Standard's enforcement date in order to confirm that modem lines were physically disconnected from the device and removed from the system;
2. Ensured an accurate and full completion of all required tasks/activities was verified and documented. The scope of work clearly defined what was meant by disconnect, removal, *etc.*, and verification of completion was the same in all cases and was documented in the same way for all sites;
3. Removed the dial-up modems in the ESPs;
4. Completed training for certain engineers and others as appropriate to reinforce the concept of ESPs and what requirements are in scope for NERC-CIP compliance. The training included the correct process for accessing and managing equipment inside an ESP; and
5. Updated the war dialing process to ensure the scan list is reviewed and approved by appropriate stakeholders for accuracy and completeness prior to initiation of the scan, and

⁷ See 18 C.F.R § 39.7(d)(7).

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 6

included in the process a step for ensuring the results from the approval were also reviewed and approved by appropriate stakeholders.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted supporting documents of completion of this Mitigation Plan.

WECC verified completion of the Mitigation Plan for CIP-005-1 R2 and notified URE in a letter.

CIP-006-3c R1 (WECC201102887)

The purpose of Reliability Standard CIP-006-3c provides: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-006-3c R1 provides in pertinent part:

R1. Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:

R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

CIP-006-3c R1 has a "Medium" VRF and a "Severe" VSL.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 7

URE submitted a Self-Report stating that it had discovered that an employee had gained unescorted access into a PSP on three dates spanning a two month period. Seventeen days after submitting the Self-Report, WECC conducted a phone interview with URE to discuss the incident, and URE confirmed that the employee was dispatched to the substation control building to respond to a service call. Upon arrival, the employee realized his access card was deactivated for failing to retake the required NERC CIP training before the annual expiration date. To gain access, the employee entered the substation by using an access card belonging to a different employee. Once the employee gained access to the PSP, he did not document entry of his arrival, nor was he provided with continuous escorted access while inside the facility. The employee gained unauthorized access on three occasions, was not escorted in any of the three instances, and failed to document the time of entry and exit as per URE's visitor's escort procedures.

Based on the record, WECC determined URE failed to ensure appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls, in violation of CIP-006-3c R1.4. In addition, WECC determined URE failed to ensure that a visitor was escorted and signed-in per URE's visitor escort procedure, in violation of CIP-006-3c R1.6.

WECC determined the duration of the violation to be from the date the violation first occurred, through present.⁸

WECC determined that this violation did not pose a serious or substantial risk and posed a minimal risk to the reliability of the BPS because although the employee without authorized unescorted access to the substation visited the facility on three occasions without being escorted and did not document time of entry and exit as per URE's procedures, the risk to the BPS was reduced by the fact that the employee had prior training (albeit expired) and a PRA. In addition, the CCAs at the facility in scope require the use of a security token prior to obtaining access. Furthermore, visitor access within the substation is monitored 24 hours, 7 days a week by logging and alerting that is reviewed at URE's security center.

Status of Mitigation Plan

URE's Mitigation Plan to address its violation of CIP-006-3c R1 was submitted to WECC on November 16, 2011 with a proposed completion date of December 1, 2012. The Mitigation Plan was accepted by

⁸ All mitigating activities related to this violation are scheduled for completion by December 1, 2012.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 8

WECC on December 13, 2011 and approved by FERC on April 19, 2012.⁹ The Mitigation Plan for this violation was submitted as non-public information to FERC on April 20, 2012 in accordance with FERC orders.

According to the Mitigation Plan, URE agreed to:

1. Install additional access control measures at its CIP critical facilities to enhance security and compliance with CIP-006;¹⁰
2. Install biometric readers (for dual authentication) and anti-tailgating technology at the primary and backup control centers. The readers serve as an additional security measures and are monitored at security control centers;
3. Conduct quarterly audits of all CIP critical facilities to confirm compliance with CIP physical access requirements. A standardized spot audit checklist form is used to capture these activities;¹¹
4. Complete a review of NERC physical access compliance requirements by the supervisor whose personnel were involved in the CIP-006 violation. The review was provided during a meeting and included escort procedures, logging and the non-sharing of access cards, and was completed;
5. Include supervisors in the automatic 45-day email notification related to their subordinates' NERC training expiration, and in an automatic 30-day reminder email;¹² and
6. Coordinate among security and IT departments on the quarterly distribution of physical and cyber security awareness information per CIP-004 R1 awareness of sound physical security

⁹ NERC received the Mitigation Plan on March 23, 2012.

¹⁰ According to the Mitigation Plan, some of these activities were already completed.

¹¹ According to the Mitigation Plan, some of these activities were already completed.

¹² In addition, the supervisor sends out an email reminder to the cardholder, their supervisor, and a copy to a manager on the day prior to the expiration of the access, stating that the cardholder's access will be terminated unless the course is completed before the deadline. The supervisor's notification will ensure that employees fulfill their annual training requirement and maintain unescorted access privileges to NERC facilities. According to the Mitigation Plan, these activities were completed.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 9

practices/access control, and on the reinforcement of CIP-006 specific compliance requirement.¹³

URE agreed to submit a certification of Mitigation Plan completion for CIP-006-3C R1 upon completing all activities included in this Mitigation Plan.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed¹⁴

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, October 26, 2009 and August 27, 2010 Guidance Orders,¹⁵ the NERC BOTCC reviewed the NOCV and supporting documentation on May 7, 2012. The NERC BOTCC approved the NOCV, including WECC's assessment of a one hundred sixty-two thousand two hundred dollar (\$162,200) financial penalty against URE based upon WECC's findings and determinations. In approving the NOCV, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. Mitigating factors:
 - a. URE self-reported the violations;
 - b. WECC reviewed URE's internal compliance program (ICP);
 - c. URE was cooperative throughout the process;
 - d. URE did not fail to complete any applicable compliance directives;
 - e. There was no evidence of any attempt by URE to conceal the violations;
 - f. There was no evidence that URE's violations were intentional; and
 - g. URE did not have a repeat violation history of CIP-006-3c R1.

¹³ According to the Mitigation Plan, these activities were completed.

¹⁴ See 18 C.F.R. § 39.7(d)(4).

¹⁵ *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).

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 10

2. Aggravating factors:
 - a. WECC determined that this is URE's second violation of CIP-005-1 R2.
3. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the NOCV and believes that the assessed penalty of one hundred sixty two thousand two hundred dollars (\$162,200) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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 Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP 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, certain Regional Entity investigative files, Registered Entity sensitive business information 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 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.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 11

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:

- a) WECC's Notice of Confirmed Violation and Proposed Penalty or Sanction for CIP-005-1 R2 and CIP-006-3c R1, included as Attachment a;
- b) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction, included as Attachment b;
- c) URE's Self-Report for CIP-005-1 R2, included as Attachment c;
- d) URE's Mitigation Plan for CIP-005-1 R2, included as Attachment d;
- e) URE's Certification of Mitigation Plan Completion for CIP-005-1, included as Attachment e;
- f) WECC's Verification of Mitigation Plan Completion for CIP-005-1 R2, included as Attachment f;
- g) URE's Self-Report for CIP-006-3c R1, included as Attachment g; and
- h) URE's Mitigation Plan for CIP-006-3c R1, included as Attachment h;

A Form of Notice Suitable for Publication¹⁶

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

¹⁶ See 18 C.F.R § 39.7(d)(6).

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 12

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 North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560</p> <p>David N. Cook* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 644-8047 (202) 644-8099 – facsimile david.cook@nerc.net</p> <p>Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz</p>	<p>Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça Attorney North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 644-8052 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net</p> <p>Christopher Luras* Manager of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz</p>
--	---

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 13

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6855
(801) 883-6894 – facsimile
CWhite@wecc.biz

Sandy Mooy*
Associate General Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 819-7658
(801) 883-6894 – facsimile
SMooy@wecc.biz

*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.

NERC Notice of Penalty
Unidentified Registered Entity
May 30, 2012
Page 14

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/s/ Rebecca J. Michael

Rebecca J. Michael
Associate General Counsel for Corporate
and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability
Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 644-8052
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

David N. Cook
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 644-8047
(202) 644-8099 – facsimile
david.cook@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments