

November 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. NP13-_-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's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).²

This Notice of Penalty is being filed with the Commission because, based on information from the Western Electricity Coordinating Council (WECC), URE does not dispute the violation³ of CIP-007-1 R6 and the proposed sixty-two thousand five hundred dollar (\$62,500) penalty to be assessed to URE. Accordingly, the violation identified as NERC Violation Tracking Identification Number WECC201102890 is a Confirmed Violation, as that term is defined in the NERC Rules of Procedure and the CMEP.

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
November 30, 2012
Page 2

Statement of Findings Underlying the Violation

This Notice of Penalty incorporates the findings and justifications set forth in the Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV), 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 (2012), 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
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-1660	WECC201102890	CIP-007-1 ⁴	R6	Medium ⁵	\$62,500

CIP-007-1 R6

The purpose statement of Reliability Standard CIP-007-1 provides: "Standard CIP-007 requires Responsible Entities⁶ 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 R6 provides in pertinent part:

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

⁴ This violation spans versions 1 through 3 of the Standard. For ease of reference, CIP-007-1 will be used throughout the remainder of this document.

⁵ CIP-007-1 R6, R6.4 and R6.5 each have a "Lower" Violation Risk Factor (VRF); CIP-007-1 R6.1, R6.2 and R6.3 each have a "Medium" VRF. WECC determined the violation was related to R6.1, and therefore a "Medium" VRF is appropriate.

⁶ Within the text of Standard CIP-007, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, TO, TOP, GO, GOP, LSE, NERC, and Regional Reliability Organizations.

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

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

CIP-007-1 R6.1 has a “Medium” Violation Risk Factor (VRF) and a “Severe” Violation Severity Level (VSL).

URE self-reported a violation of CIP-007-1 R6. During an internal review of network devices a few months earlier, URE identified a segment of network equipment residing within multiple Electronic Security Perimeters (ESPs) that failed to have implemented and documented organizational processes, as well as the technical and procedural mechanisms required for monitoring security events. Specifically, URE discovered over 1,000 devices that did not have security monitoring as required by R6.1. URE determined it was technically infeasible to comply with this requirement for 88% of the total devices discovered as noncompliant.

WECC subject matter experts (SMEs) reviewed URE’s Self-Report and associated requests for Technical Feasibility Exceptions (TFEs). WECC approved URE’s CIP-007 R6 TFEs, resulting in the remaining 12% of the total Cyber Assets in scope of URE’s noncompliance. These devices include workstations, servers and network devices. The SME determined that URE’s failure to implement security monitoring on these devices was a result of inadvertently relying on the anti-virus and host intrusion detection system to perform the security monitoring measures. Therefore, the SME determined that URE was in violation of CIP-007-1 R6 for failing to implement security monitoring controls on Cyber Assets for which it was technically feasible to do so. The SME forwarded the findings to WECC Enforcement for review and determination.

WECC Enforcement reviewed URE’s Self-Report and the SME’s findings. WECC Enforcement determined that URE was in violation of CIP-007-1 R6.1 for failing to ensure that Cyber Assets located in URE’s control center, facilities and control systems had mechanisms for monitoring system events related to cyber security. The cause for the workstations not being monitored was a configuration failure due to URE’s reliance on anti-virus and its intrusion detection system. The workstations were not configured to log system events related to cyber security. For the servers, the logging agent stopped and was not configured properly after replacement. Some of the network devices were logging but not set up to send alerts. Finally, the remaining network devices had security monitoring implemented, but URE did not document the organizational process being performed.

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

WECC determined that URE had a violation of CIP-007-1 R6.1 for failing to document its organizational process for monitoring for security events on all Cyber Assets within its ESPs.

WECC determined the duration of the violation was from the date the Standard became mandatory and enforceable for URE through the date when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, failure to implement security controls to monitor cyber security system events could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to Critical Cyber Assets essential to the operation of the BPS, thereby potentially negatively impacting the BPS. In this instance, URE failed to implement security monitoring on Cyber Assets for a period of 31 months. These Cyber Assets consisted of work stations, servers and network devices. As compensating measures, the assets within the scope of the violation are located and protected within identified ESPs and Physical Security Perimeters and have technical and procedural mechanisms for control of electronic and physical access. For instance, URE logs and monitors physical and electronic access by authorized users 24-hours-a-day and seven days a week. Further, URE requires usernames and passwords on all Cyber Assets and uses security software to monitor any changes made within the ESP.

Regional Entity's Basis for Penalty

WECC assessed a penalty of sixty-two thousand five hundred dollars (\$62,500) for the referenced violation. In reaching this determination, WECC considered the following factors: (1) URE self-reported the violation; (2) URE took voluntary corrective action to remediate this violation; (3) WECC reviewed URE's internal compliance program (ICP) and considered it a mitigating factor in the penalty determination; (4) there were no aggravating factors to warrant a higher penalty; (5) URE did not have any relevant negative compliance history; (6) this violation posed a moderate risk to the reliability of the BPS and did not pose a serious or substantial risk to the BPS; (7) URE was cooperative throughout the compliance enforcement process; (8) URE did not fail to complete any applicable compliance directives; (9) there was no evidence of any attempt by URE to conceal the violation; and (10) there was no evidence that URE's violation was intentional.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of sixty-two thousand five hundred dollars (\$62,500) is appropriate and bears a reasonable relation to the seriousness and duration of the violation.

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

Status of Mitigation Plan⁷

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to WECC on September 21, 2011. The Mitigation Plan was accepted by WECC on October 7, 2011 and approved by NERC on November 11, 2011. The Mitigation Plan for this violation is designated as WECCMIT005990 and was submitted as non-public information to FERC on November 11, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update its existing process for identification and remediation of systems that stop monitoring as a result of system or other operational issues and update its system to clarify requirements and timelines for notification and documentation;
2. Complete and submit a TFE Part A for the devices where logging and automated monitoring is not technically feasible. This requirement includes submitting a total of four TFEs, one for each device type;
3. Complete on-boarding and support full monitoring and analysis of all network devices;
4. Complete and submit a TFE Part B for the four TFEs submitted, once notifications of acceptance of the TFE Part As are received from WECC;
5. Complete an assessment (including testing and selection) of logging/monitoring options for workstations; and
6. Complete implementation of the logging/monitoring solution identified above.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of its completion of its Mitigation Plan to WECC.

WECC verified that it had reviewed URE's evidence and that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁸

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,⁹ the NERC

⁷ See 18 C.F.R. § 39.7(d)(7).

⁸ See 18 C.F.R. § 39.7(d)(4).

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

BOTCC reviewed the NOCV and supporting documentation on November 5, 2012. The NERC BOTCC approved the NOCV, including WECC's assessment of a sixty-two thousand five hundred dollars (\$62,500) 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 violation at issue.

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

1. URE self-reported the violation;
2. WECC reviewed URE's ICP and considered it a mitigating factor in the penalty determination;
3. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty, as discussed above;
4. the violation constituted URE's first occurrence of violation of the subject NERC Reliability Standard requirement;
5. WECC determined that the violation did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
6. WECC reported that URE was cooperative throughout the compliance enforcement process;
7. there was no evidence of any attempt by URE to conceal the violation; and
8. there was no evidence that URE's violation was intentional.

For the foregoing reasons, the NERC BOTCC approved the NOCV and believes that the assessed penalty of sixty-two thousand five hundred dollars (\$62,500) is appropriate for the violation 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.

⁹ *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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

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. The public release of this information could compromise system security due to its inclusion of information regarding: the identification of the types and classes of vulnerabilities that this entity must continuously guard against; a description of system architecture and configuration, facilities, and other assets that, if disclosed, would assist in the planning of a targeted, vectored attack; and other sensitive data.

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.

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) URE's Response to the Notice of Alleged Violation and Proposed Penalty or Sanction for CIP-007-1 R6 (WECC201102890), included as Attachment a;
- b) URE's Self-Report for CIP-007-1 R6 (WECC201102890), included as Attachment b;
- c) URE's Mitigation Plan for CIP-007-1 R6 (WECC201102890), included as Attachment c;
- d) URE's Certification of Mitigation Plan Completion for CIP-007-1 R6 (WECC201102890), included as Attachment d; and
- e) WECC's Verification of Mitigation Plan Completion for CIP-007-1 R6 (WECC201102890), included as Attachment e.

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

A Form of Notice Suitable for Publication¹⁰

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

¹⁰ See 18 C.F.R § 39.7(d)(6).

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

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>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) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net</p>
<p>Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@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>Christopher Luras* Director 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>
<p>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</p>	<p>Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile RArredondo@wecc.biz</p>

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

*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
November 30, 2012
Page 11

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) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments