May 29, 2014

VIA ELECTRONIC FILING

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 (URE), FERC Docket No. NP14-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] 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 Western Electricity Coordinating Council (WECC), URE does not dispute the violations[3] of CIP-007-1 R5 and R6 and the proposed ninety-eight thousand five-hundred dollar ($98,500) penalty to be assessed to URE. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers

---

[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 (2013). *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.

WECC2013012597 and WECC2013012598 are being filed in accordance with 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 (NOCV) issued 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 (2013), 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-2292	WECC2013012597	CIP-007-1	R5; R5.1.2	Lower	$98,500
			WECC2013012598	CIP-007-1	R6	Medium	

<u>CIP-007-1 R5 (R5.1.2)</u>
The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities 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)."

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

***

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

***

CIP-007-1 R5 has a "Lower" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Report stating that it was in violation of CIP-007 R5. Specifically, for over 30 workstations, URE failed to establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.

URE reported that it discovered the violation during a review of its CIP compliance program. During this review, it performed site visits to confirm that its asset lists and drawings were up to date. The workstations affected by the violation were used in the normal operation and maintenance of URE's Supervisory Control and Data Acquisition (SCADA) system, energy management system (EMS), and Remedial Action Scheme (RAS) system.

URE determined that the violation was a result of a server not being configured properly to receive logs of sufficient detail from the workstations at issue. Because URE failed to ensure the appropriate technical and procedural controls were established to generate logs of sufficient detail on these workstations, URE failed to create a historical audit trail of individual user access for a minimum of 90 days.

WECC determined that URE had a violation of CIP-007-1 R5 (R5.1.2) for failing to ensure that the workstations were generating logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of 90 days.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through 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, URE's failure to create historical audit trails of individual user account access could have aided in losing visibility to the affected workstations. Without logging procedures and controls, URE would not have been able to identify or receive alerts for forced attacks, multiple bad password attempts, or irregular logons to these workstations. If any of these events were not noticed or investigated, an unauthorized person could have gained access to URE's SCADA, EMS, or RAS systems.

However, the SCADA, EMS, and RAS systems were protected from unauthorized access by URE's authentication systems, which required a token and password before allowing log-in and access. In addition, URE had personnel responsible for monitoring network activity in real time. These personnel were trained to recognize and respond to anomalous events. In order to access the devices affected by the violation, personnel must have been on-site. The Physical Security Perimeters (PSPs) in which the affected devices were located only allowed access to authorized personnel. Further, URE's Physical Access Control System (PACS) would have discovered unauthorized access to the PSPs.

No unauthorized access is known to have occurred.

<u>CIP-007-1 R6</u>
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.

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.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Report stating that it was in violation of CIP-007-1 R6. Specifically, URE failed to implement automated tools or organizational process controls to monitor system events related to cyber security for the same workstations described in the violation of CIP-007-1 R5 above. URE determined that the violation was a result of a server not being configured properly to receive logs of system events related to cyber security from the workstations.

Following the Self-Report, URE conducted an expanded extent-of-condition review. Following this review, URE discovered that approximately 150 servers and workstations and approximately 50 network switches were not forwarding logs to the log monitoring servers.

Because URE failed to ensure that the workstations had automated tools or organizational process controls to monitor system events, URE did not maintain logs of system events related to cyber security (R6.3) and did not retain such logs for 90 days (R6.4).

WECC determined that URE had a violation of CIP-007-1 R6 for failing to implement automated tools or organizational process controls to monitor system events that are related to cyber security.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until mitigated.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE’s failure to implement automated tools or organizational process controls to monitor system events related to cyber security could have aided in potentially losing visibility to the workstations. Without logging procedures and controls, URE would not have been able to identify or receive alerts for forced attacks, multiple bad password attempts, or irregular logons to workstations. If any of these events were not noticed or investigated, an unauthorized person could have gained access to URE's SCADA, EMS, or RAS systems.

However, the SCADA, EMS, and RAS systems were protected from unauthorized access by URE's authentication systems, which required a token and password before allowing log-in and access. In addition, URE had personnel responsible for monitoring network activity in real time. These personnel were trained to recognize and respond to anomalous events. In order to access the devices affected by the violation, personnel must have been on-site. Further, the PSPs in which the affected devices were located only allowed access to authorized personnel; URE's PACS would have discovered unauthorized access to the PSPs.

No unauthorized access is known to have occurred.

Regional Entity's Basis for Penalty
WECC assessed a penalty of ninety-eight thousand five hundred dollars ($98,500) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC determined that URE's compliance history warranted an aggravation of the monetary penalty;
2. URE self-reported the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of ninety-eight thousand five hundred dollars ($98,500) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[4]

CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC stating it had been completed. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to perform an extent-of-condition review, remediate the out-of-compliance state for the applicable systems, and verify that the systems were logging user account activity.

URE certified that the above Mitigation Plan requirements were completed. WECC is in the process of verifying the completion of URE's Mitigation Plan.

CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. address the non-compliant condition on the identified devices and systems;
2. assess options for how best to determine whether all CIP assets are consistently and effectively generating logs on an ongoing basis;
3. develop and implement a process for detecting and correcting situations where systems are not creating or forwarding logs;
4. identify and train personnel that will be responsible for utilizing the new process; and
5. complete and publish all documentation and procedures associated with the Mitigation Plan.

[4] *See* 18 C.F.R § 39.7(d)(7).

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

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,[6] the NERC BOTCC reviewed the NOCV and supporting documentation on May 5, 2014. The NERC BOTCC approved the NOCV, including WECC's assessment of a ninety-eight thousand five-hundred dollar ($98,500) 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 violations at issue.

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

1. WECC determined that URE's compliance history warranted an aggravation of the monetary penalty, as discussed above;
2. URE self-reported the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violation which WECC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. 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 ninety-eight thousand five hundred dollars ($98,500) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

---

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *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).

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.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

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 North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 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 Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz 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 rarredando@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.	Chris Luras* Director of Compliance Risk Analysis & 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

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

Sonia C. Mendonça
Associate General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments