PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

November 30, 2016

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, FERC Docket No. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), with information and details regarding the nature and resolution of the violations[2] discussed in detail in the Notice of Confirmed Violation (NOCV), 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)).[3]

NERC is filing this Notice of Penalty with the Commission because Midwest Reliability Organization (MRO) has issued an NOCV to resolve all outstanding issues arising from MRO's determination and findings of three violations of Critical Infrastructure Protection (CIP) Reliability Standards.

---

[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 (2016). *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] 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.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

NERC is filing this Notice of Penalty with the Commission because, based on information from MRO, URE does not dispute the violations and the one hundred forty-two thousand dollar ($142,000) penalty assessed to URE.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the NOCV issued by MRO. 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 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV. Further information on the subject violations is set forth in the NOCV and herein.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
MRO2015014792	CIP-002-3	R3	High/ Severe	CA	Moderate	$142,000
MRO2015014793	CIP-005-1	R1	Medium/ Severe			
MRO2015014794	CIP-007-1	R1.1 R1.3				

MRO2015014792 CIP-002-3 R3 - OVERVIEW

MRO determined that URE did not develop a complete list of all the required Critical Cyber Assets (CCAs). Specifically, URE did not list certain Inter-Control Center Communications Protocol (ICCP) servers as CCAs. The cause of this violation was URE's reliance upon a third-party vendor that incorrectly advised URE that locating the ICCP servers outside of the Electronic Security Perimeter (ESP) was prudent and would improve security.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, the ICCP servers were essential to the operation of the primary and backup control centers. URE used them to exchange real-time information for

essential functions including: generator set point values; Special Protection System status; breaker status; and megawatt line flows between URE and its Reliability Coordinator. If the generator set point data is not available to the URE control center or the URE supervisory control and data acquisition (SCADA) data is not available to its Reliability Coordinator, there could be an adverse effect on the reliable operation of the BPS.

Nevertheless, while URE did not classify the ICCP servers as CCAs, it was protecting the servers as if they were CCAs. Specifically: 1) the servers were located inside of a Physical Security Perimeter (PSP), and any individuals with logical or physical access had each undergone a background check; 2) any significant change to the servers met the requirements of URE's change control and configuration management program; 3) URE patched the servers and evaluated all applicable security patches monthly; 4) URE utilized account management techniques including password complexity and logging measures to reduce the risk of intrusion by an adversary; and 5) URE documented all active and enabled ports and services and utilized a program to monitor for unauthorized usage.

Finally, MRO reviewed network architecture. URE used firewalls to block and limit unwanted external network traffic from entering both the ICCP servers and the ESP. This reduced the potential amount of untrusted network traffic from accessing the ICCP servers and ESP. During the network review, MRO ascertained that the ICCP servers were behind a corporate firewall, yet not in a defined ESP where CCAs are required to be located. The ICCP servers were logically isolated from the ESP per vendor recommendation.

MRO determined the duration of the violation was from when URE activated the ICCP servers that were not listed as CCAs through Mitigation Plan completion.

To mitigate this violation, URE:

1. implemented new ESPs at the primary control center and at the backup control center;
2. moved the ICCP server nodes to logically migrate the ICCP servers to new segments off the control center firewalls and declared these networks as ESPs; and
3. created and implemented new Cyber Asset procedures to ensure that new devices added to an ESP are compliant with the NERC Reliability Standards.

MRO verified that URE completed all mitigation activities.

MRO2015014793 CIP-005-1 R1 - OVERVIEW

MRO determined that URE failed to meet the requirements of CIP-007-1 (test procedures) for a Cyber Asset used in the access control and monitoring of the ESP. Specifically, sampling revealed that a CCA, an Electronic Access Control and Monitoring (EACM) device, underwent a significant change, and the requisite test procedures associated with that significant change were not adequately documented. The URE procedure was incomplete and did not list the performance test steps, which led to the failure to produce sufficient evidence to demonstrate that testing was performed, the specific test steps to be performed, and the test procedures.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE performed some testing for adverse impacts to user security controls; however, it did not document all required testing. Through discussion with the URE subject matter expert, it was determined that the change made to the CCA was intended to be tracked in the security testing spreadsheet; however, the actual testing performed was not documented.

After discussions with the URE subject matter expert, MRO ascertained that URE completed user account reviews for default and administrator accounts, but not individual named user accounts.

Moreover, URE was performing other CIP user security requirements. Specifically, URE implemented technical and procedural controls to manage authentication and authorization, including tracking user access and managing password complexity rules for monitoring devices. MRO did not discover any noncompliance where URE did not perform periodic user account reviews for monitoring devices. MRO did not discover any noncompliance in situations where Cyber Assets within the ESP did not have technically feasible, automated tools or organizational process controls to monitor system events related to cyber security. Finally, MRO did not discover any noncompliance related to performing logging and managing log retention for monitoring devices.

MRO determined the duration of the violation was from when the standard became mandatory and enforceable on URE through Mitigation Plan completion.

To mitigate this violation, URE:

1. upgraded the testing software used for the devices to incorporate the Tripwire policy module for the numerous high impact Bulk Electric System (BES) Cyber Assets;
2. retired the spreadsheet legacy checklist procedure and developed and implemented new procedures; and
3. trained staff on new procedures.

MRO verified that URE completed all mitigation activities.

MRO2015014794 CIP-007-1 R1.1 & R1.3 - OVERVIEW

MRO determined that URE failed to document its testing process sufficiently to include detailed steps for account testing and to document the associated test results sufficiently. Specifically, sampling revealed that a CCA, an EACM device, underwent a significant change, and the requisite test procedures associated with that significant change were not adequately documented. The URE procedure was incomplete and did not list the performance test steps, which led to the failure to produce sufficient evidence to demonstrate that testing was performed, the specific test steps to be performed, and the test procedures.

MRO determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE performed some testing for adverse impacts to user security controls; however, it did not document all required testing. Through discussion with the URE subject matter expert, it was determined that the change made to the CCA was intended to be tracked in the security testing spreadsheet, however, the actual testing performed was not documented. After discussions with the URE subject matter expert, MRO ascertained that URE completed user account reviews for default and admin accounts, but not individual named user accounts.

Nevertheless, URE was performing other CIP user security requirements. Specifically, URE implemented technical and procedural controls to manage authentication and authorization, including tracking user access and managing password complexity rules for monitoring devices. MRO did not discover any noncompliance where URE did not perform periodic user account reviews for monitoring devices. MRO did not discover any noncompliance in situations where Cyber Assets within the ESP did not have technically feasible, automated tools or organizational process controls to monitor system events related to cyber security. Finally, MRO did not discover any noncompliance related to performing logging and managing log retention for monitoring devices.

MRO determined the duration of the violation was from when the standard became mandatory and enforceable on URE through Mitigation Plan completion.

To mitigate this violation, URE:

1. upgraded the testing software used for the devices to incorporate the Tripwire policy module for the numerous high impact BES Cyber Assets;

2. retired the spreadsheet legacy checklist procedure and developed and implemented new procedures; and
3. trained staff on new procedures.

MRO verified that URE completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Notice of Confirmed Violation, MRO has assessed a penalty of one hundred forty-two thousand dollars ($142,000) for the referenced violations. In reaching this determination, MRO considered the following factors:

1. MRO considered URE's compliance history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which MRO considered a neutral factor;
3. MRO did not consider URE's initial level of cooperation to be a mitigating factor in the initial penalty determination. Following a post-audit meeting with URE representatives, MRO noticed a significant change in the level of cooperation during the development and implementation of mitigation. MRO considered the involvement of senior management in the process as evidence of a strong commitment to the security and reliability of the BPS. Thereafter, MRO considered URE's cooperation to be a mitigating factor in the penalty determination;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations posed a moderate and not serious or substantial risk to the reliability of the BPS; and
6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, MRO determined that, in this instance, the penalty amount of one hundred forty-two thousand dollars ($142,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

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,[5] the NERC BOTCC reviewed the NOCV and supporting documentation on October 31, 2016 and approved the NOCV. 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.

For the foregoing reasons, the NERC BOTCC approved the NOCV and believes that the assessed penalty of one hundred forty-two thousand dollars ($142,000) 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.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

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

Daniel P. Skaar* President Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1731 dp.skaar@midwestreliability.org Sara E. Patrick* Vice President of Compliance Monitoring and Regulatory Affairs Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1708 se.patrick@midwestreliability.org Jackson Evans* Enforcement Attorney Midwest Reliability Organization 380 St. Peter Street, Suite 800 Saint Paul, MN 55102 (651) 855-1758 jj.evans@midwestreliability.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.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel 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 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 Leigh Anne Faugust* Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Leigh Anne Faugust
Counsel, 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.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
Midwest Reliability Organization