February 28, 2018

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. NP18-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) 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]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of two violations of the Critical Infrastructure Protection (CIP) NERC 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 (2017). *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) and 18 C.F.R § 39.7(d).

[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.

According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two million seven hundred thousand dollars ($2,700,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement 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 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

Violation(s) Determined and Discovery Method *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**
WECC2016016233	CIP-003-3	R4	Medium/ Severe	SR	Serious	$2.7M
WECC2016016234	CIP-003-3	R5	Lower/ Severe			

Background to the Violations

URE received a report of an online data exposure with data possibly associated with URE. The report came from a white hat security researcher not associated with URE. A third-party URE contractor exceeded its authorized access by improperly copying certain URE data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. The contractor failed to comply with URE's information protection program on which it was trained. While the data was on the contractor's network, a subset of live URE data was accessible online without the need to enter a user ID or password. This subset of data included over

30,000 asset records, including records associated with Critical Cyber Assets (CCAs). The records included information such as IP addresses and server host names.

The information associated with the CCAs was accessible on the Internet for a total of 70 days. URE also reviewed the system logs of the contractor and found that the logs showed unauthorized access to the URE data subset from unknown IP addresses, as well as IP addresses associated with the white hat security researcher who notified URE of the data exposure.

URE informally notified WECC of the incident and explained how URE was managing the situation. URE and WECC had multiple discussions and meetings about the situation over the next two months. Four months after it had discovered the incident, URE submitted an incident update to WECC.

Based on information from URE's incident report and WECC data requests, WECC recommended URE file Self-Reports for the issues. WECC determined URE failed to implement adequately its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. WECC also determined URE failed to implement adequately a program for managing access to protected information related to CCAs, as required by CIP-003-3 R5.

Analysis of the system logs showed that only the security researcher executed commands to view and download data. More detailed system logs would be required to determine definitively that no other third party had downloaded the data, but the short duration of the connections decreased the likelihood that additional accessing or downloading of data had occurred. To recover the exposed data, URE contacted the security researcher and requested that he securely return the data, securely delete all copies of the data from his system, and submit to URE a signed, notarized affidavit confirming that he deleted all copies of the data.

RISK COMMON TO THE VIOLATIONS

These violations posed a serious or substantial risk to the reliability of the bulk power system (BPS). The CCAs associated with the data exposure include servers that store user data, systems that control access within URE’s control centers and substations, and a supervisory control and data acquisition (SCADA) system that stores critical CCA Information. The data was exposed publicly on the Internet for 70 days. The usernames of the database were also exposed, which included cryptographic information of those usernames and passwords.

Exposure of the username and cryptographic information could aid a malicious attacker in using this information to decode the passwords. This exposed information increases the risk of a malicious attacker gaining both physical and remote access to URE's systems. A malicious attacker could use this

information to breach the secure infrastructure and access the internal CCAs by jumping from host to host within the network. Once in the network, the attacker could attempt to login to CCAs, aided by the possession of username and password information.

WECC found URE had implemented limited compensating controls to reduce the risk associated with a malicious actor gaining access to its system during the noncompliance. URE did not classify the data as CIP-protected information because it was on a pre-production server, nor were there any controls in place to prevent the contractor from taking the data off premises and putting it on their own Internet-facing network. URE had implemented simple-character usernames similar to the usernames that were publicly exposed. In addition, URE did not implement any preventive or detective controls. URE only discovered the data exposure because of an external white hat security researcher who found the publicly accessible data on the Internet.

URE has three firewalls between the external network and the assets inside the Electronic Security Perimeter that make it difficult for a malicious actor to access URE's CCAs. Based on the controls WECC analyzed, there was lower probability that this instance of noncompliance would have caused an impact to the reliability of the BPS at the time of its occurrence. Nevertheless, there is no reasonable assurance that during the time the data was exposed on the Internet, it was not already used by a malicious actor – or collected by such an actor – to access URE's network and install an application that can cause the potential harm in the future. The additional sanction described below is intended to address this residual risk.

MITIGATION ACTIVITY COMMON TO THE VIOLATIONS

URE submitted identical Mitigation Plans to address the referenced violations. To mitigate these violations, URE:

1. Required the vendor to shut down their software development server, thereby ending the data exposure;
2. Performed three different forensic analyses to verify that only the security researcher accessed the data during the time of the exposure;
3. Required the security researcher to provide the data to the IT department, delete the data from his computer, and attest in an affidavit that these items were complete;
4. Removed vendor access to the asset management database in the datacenter. To allow vendors to perform development work on projects, URE implemented a process whereby an authorized URE employee must copy the source code from the asset management database and securely transfer it to the software development vendor. Upon work

completion, the vendor would then securely transfer the new version of code to an authorized URE employee who would load it back onto the asset management database;

5. Changed access controls to the database. URE also deployed a suite program to provide policies and controls to prevent confidential-Bulk Electric System (BES) Cyber System Information or restricted-BES Cyber System Information classified emails and attachments from being sent to outside email addresses;

6. Improved security controls for vendor management by requiring vendors to take information security and privacy awareness training annually, implementing a new vendor remote access platform, and enhancing policies, background checks, and contract language for vendor employees; and

7. Classified all BES Cyber System Information for both production and non-production assets.

URE certified that it had completed its Mitigation Plan, and WECC verified that URE had completed all mitigation activities.

VIOLATION DESCRIPTIONS

CIP-003-3 R4 - OVERVIEW

WECC determined that URE did not adequately implement its program to identify, classify, and protect information associated with CCAs, as required by CIP-003-3 R4. Specifically, in the above described incident, WECC found that URE failed to adequately implement the following areas of its program to identify, classify, and protect information associated with CCAs:

1. URE failed to identify and classify the information used in the system in accordance with its information protection policy. URE stated it did not classify in accordance with its policy because the information was part of a pre-production asset management system. Even though the data was in a pre-production system, it is live CCA Information, and URE was required to implement a program to identify, classify, and protect this information.

2. Due to URE's failure to classify the information, URE also failed to provide the proper protections during storage and transmission, distribution, and duplication, in accordance with its policy.

3. URE failed to designate the system and the contractor's network IP as a CCA Information approved storage location and store CCA Information in an approved location.

4. URE failed to ensure that personnel handling CCA Information adhered to URE's protection measures.

5. URE failed to activate its existing policies or procedures for sharing protected information with third parties before information was disseminated, either electronically or physically, in accordance with its policy.

The cause of this violation was URE's failure to apply its information protection program to the CCA Information in its pre-production environment.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 590 days, from the date the third-party contractor exposed the information on the Internet, through when URE completed classifying all CCA Information for production and non-production assets. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

CIP-003-3 R5 - OVERVIEW

WECC determined that URE did not implement a program for managing access to protected CCA Information, as required by CIP-003-3 R5. Specifically, in the above described incident, WECC found that URE failed to ensure that the contractor protected the CCA Information when it improperly copied the data from URE's network environment to the contractor's network environment, where it was no longer subject to URE's visibility or controls. In response to a data request, due to the fact that the contractor copied the data to an unapproved location, URE stated that the security controls for the contractor's storage location were not understood or documented. WECC found that URE did not understand or document the security controls at the contractor's location before it released information to the contractor, and afterward, when the data was exposed to the Internet, it failed to adequately implement its program for managing access.

The cause of this violation was URE's failure to ensure its contractor followed its information protection program and procedures on which the contractor was trained.

WECC determined that this violation posed a serious and substantial risk to the reliability of the BPS.

WECC determined the duration of the violation to be approximately 80 days, from the date the third-party contractor exposed the information on the Internet, through when the white hat security researcher deleted all remaining electronic copies of data and screen shots from his hard drive and sanitized his device to prevent future access. WECC cannot confirm that another third party did not capture and retain possession of the exposed data.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two million seven hundred thousand dollars ($2,700,000) for the referenced violations as well as a non-monetary sanction. As an additional sanction designed to reduce the opportunities for a malicious actor to use the exposed data, WECC required URE to set its relevant CIP passwords-remembered to "all" or the maximum the system will remember to prevent passwords from being used more than once, or to maximize the frequency for which a password may be used.

In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE had an internal compliance program at the time of the violation;
3. URE self-reported the violations;
4. URE was not fully transparent and forthcoming with all pertinent information detailing the data exposed in the incident. Specifically, URE did not provide WECC initially with all the data fields exposed in the incident;
5. the violations posed a serious and 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, WECC determined that, in this instance, the penalty amount of two million seven hundred thousand dollars ($2,700,000) 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 Settlement Agreement and supporting documentation on February 6, 2018, and approved the Settlement Agreement. In approving the Settlement Agreement, 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 Settlement Agreement and believes that the assessed penalty of two million seven hundred thousand dollars ($2,700,000) 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:

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Steve Goodwill* Vice President and General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6857 (801) 883-6894 – facsimile sgoodwill@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 rarredondo@wecc.biz Heather Laws* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@wecc.biz	Sonia C. Mendonça* Vice President, Acting General Counsel and Corporate Secretary, 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 Director of Enforcement Oversight 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 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

*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.	

Conclusion

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

Respectfully submitted,

/s/ Leigh Anne Faugust

Sonia C. Mendonça
Vice President, Acting General Counsel and Corporate Secretary, and Director of Enforcement
Edwin G. Kichline
Senior Counsel and Director of Enforcement Oversight
Leigh Anne Faugust
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.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council