PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

October 31, 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) 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 four violations of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to other remedies

[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] *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.

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 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement. Further information on the subject violations is set forth in the Settlement Agreement.

*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
WECC2014013506	CIP-002-3	R4	Lower/ Moderate	SC	Moderate	$250,000
WECC2014013873	CIP-005-3a	R1	Medium/ Severe	SR		
WECC2014014531	CIP-006-3c	R2		SR		
WECC2015014704	CIP-007-3a	R8		SC		

WECC2014013506 CIP-002-3 R4 - OVERVIEW

WECC determined that URE failed to approve its Critical Cyber Assets (CCAs) list during one calendar year. WECC also determined that URE completed its annual inventory, but that the CIP senior manager failed to review and approve the list within the required timeframe.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). An inaccurate list of CCAs could potentially leave Cyber Assets that are essential to the operation of an identified CCA unknown and unprotected. Failing to protect these essential Cyber Assets could lead to misuse or compromise of the Cyber Asset, leading to

a negative impact on the associated CCA. While URE implemented alternative controls to prevent unauthorized access to CCAs, including a seven-step process for updating the CCA list and ongoing updates through the change control process, URE's measures failed in this instance. URE did not discover that it had failed to approve its CCA list until URE was preparing for its Self-Certification submittal. Nevertheless, URE completed the annual inventory on time and submitted it to the CIP senior manager for approval. The CIP senior manager failed to complete this task within the required period.

WECC determined the duration of the violation to be the entire calendar year for the certain missed compliance period.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Perform a process review to identify and clarify the communication and work flow requirements;
2. Test the process to ensure the work flow and communication requirements;
3. Draft and implement an automated task to meet the process requirements; and
4. Test and validate the automated task notification and functionality.

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

WECC2014013873 CIP-005-3a R1 - OVERVIEW

WECC determined that URE failed to identify and document all access points to the Electronic Security Perimeter (ESP). WECC determined that URE failed to provide an access point all the required protective measures and failed to maintain documentation of all electronic access points to the ESP.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE connected one switch in the test environment to the control center ESP, creating an undocumented access point into that ESP. Failing to identify an ESP access point and afford it with CIP protections could allow a malicious person to discover the access point by scanning URE or by gaining physical access to the device. The malicious person could then launch a malware attack on the switch to attempt to gain logical access to the device. If the attack were successful, the malicious person could then use the device to send attack packets into the ESP, which houses the Supervisory Control and Data Acquisition (SCADA), Energy Management System, and Remedial Action Scheme system, and potentially gain control of one of those systems, thereby compromising up to five pieces of Bulk Electric System (BES) equipment. Additionally, the device was part of a test network. If

vulnerabilities are introduced into the test network, the vulnerabilities could spread from the test environment to the control center ESP.

Nevertheless, URE implemented both preventive and detective controls. As preventive controls, the switch was located inside an area that requires key card access, and URE uses anti-virus software in the ESP to monitor traffic. As additional preventive measures, URE uses an intrusion prevention system, which also monitors traffic for malware and could stop a malware attack. Further, the applicable devices were contained in a secure and locked facility only accessible by SCADA technicians who all have NERC CIP logical and physical access. As detective measures, URE has personnel in the control center around the clock, who would detect any change in generation. In addition, URE uses event logging and monitoring of devices in the ESP, which could have detected repeated access attempts.

WECC determined the duration of the violation to be from when URE installed the switch connecting the test environment and control center through when URE removed the switch from the ESP.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Evaluate existing processes using lessons learned from this instance, and others, to determine if there are sections that need to be strengthened or added;
2. Implement and operationalize any design modifications identified above, including workforce training;
3. Implement technology and procedures to continuously baseline assets located within ESP and detect deltas due to changes, strengthening design of the control;
4. Identify and implement a process to evaluate the effectiveness of the training of all personnel performing work within these environments, strengthening operation of the control;
5. Observe performance and collect evidence for a 90-day period to ensure its effectiveness prior to closing out the Mitigation Plan;
6. Implement CIP Version 5 procedure for ports and service procedure, change management procedure, and signage controls on BES Cyber Assets;
7. Implement the change management procedure and track controls to trigger updates to inventory list and ESP drawings;
8. Implement CIP Version 5 procedure for operationalizing the new signage controls on BES Cyber Assets;
9. Operationalize the signage controls on BES Cyber Assets;
10. Operationalize the change management procedure into work processes;
11. Evaluate effectiveness of signage controls on BES Cyber Assets;
12. Evaluate effectiveness of change management procedure controls for updating inventory list and ESP drawings; and

13. Modify, if necessary, and re-publish ports and services procedures and change management procedures.

WECC2014014531 CIP-006-3c R2 - OVERVIEW

WECC determined that URE failed to ensure that its Cyber Assets that authorize and/or log access to the Physical Security Perimeters (PSPs) be afforded the protective measures specified in CIP-006-3c.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Software was implemented on URE's Physical Access Control System (PACS) servers; anyone with the appropriate access to this software could grant and revoke access to all of URE's PSPs. As a result, a larger number of personnel had the ability to provision access to PSPs. This could allow a malicious, unauthorized individual to provision unauthorized personnel into any PSP. Once access was granted, the unauthorized individual could physically destroy or harm CCAs, attempt to logically access devices and modify configurations, or input a virus with a universal serial bus (USB) device. These CCAs were in this increased vulnerable state for an extended period.

Nevertheless, URE implemented preventive and detective controls. Specifically, URE's primary and back-up control centers are staffed around the clock, thereby reducing the likelihood of malicious personnel destroying or manipulating CCAs. Additionally, URE implemented strong username and password login restrictions to all CCAs, thereby reducing the likelihood of malicious personnel gaining unauthorized electronic access to these devices. In addition, URE uses a corporate-wide anti-virus solution to prevent the introduction and spread of a virus implanted with a USB device. As a corrective control, URE implemented backups of its servers so they could be restored to a trusted state.

WECC determined the duration of the violation to be from when URE implemented a certain software that began provisioning access to the PSPs without the required protections through when URE enhanced the specific software's functionality and security with the required protections.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Demonstrate compliance of system security to meet best business practice and CIP compliance; and
2. Qualify scope of PACS categorization relative to NERC CIP Version 5.

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

WECC2015014704 CIP-007-3a R8 - OVERVIEW

WECC determined that URE failed to perform a Cyber Vulnerability Assessment (CVA) of all Cyber Assets within the ESP at least annually.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE failed to perform a CVA of all Cyber Assets within the ESP. Specifically, URE would sample like devices while performing the CVA and would not perform a CVA of all applicable devices. Failure to conduct a CVA could allow cyber vulnerabilities to go undetected, potentially allowing for exploitation by a malicious person to launch cyber-attacks against CCAs essential to the operation of BES.

URE implemented both preventive and detective controls. As preventive controls, URE's network employs defense in depth that monitors incoming traffic to the network. URE's firewalls use access control lists to permit only traffic from known IP addresses, denying all other traffic. The firewalls also require multi-factor authentication for remote users. URE also uses electronic and physical access controls, requiring PINs and access cards in order to gain access into the PSPs containing CCAs. If access to the PSP were obtained by a malicious person, URE utilizes around-the-clock security personnel. As detective controls, URE uses logging on its devices, including firewalls, to alert unauthorized access attempts. In addition, URE uses alarms to alert for changes in load and URE did perform a CVA on some assets, but not for all required assets.

WECC determined the duration of the violation to be from the beginning of the calendar year in which URE first failed to complete a CVA through the end of the last year when URE completed a CVA that did not include all Cyber Assets.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. Determine involvement of other processes and procedures;
2. Develop process flow to reflect new CIP standard and links to other identified processes and procedures;
3. Complete a CVA for the previous calendar year to include previously missed Cyber Assets residing within established ESPs;
4. Revise the procedure to reflect lessons learned and feedback from stakeholders, as well as the new CIP Version 5 vulnerability assessment requirements;
5. Pilot the new process;
6. Modify the process and procedures; and
7. Approve and published processes and procedures as appropriate.

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

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's CIP compliance history to be an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violations which WECC considered a mitigating factor;
3. URE voluntarily self-reported two of the violations; however, URE did not receive mitigating credit for one of the violations because the Self-Report was submitted during the Self-Certification period;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. all four violations posed a moderate risk to the reliability of the BPS; 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 two hundred fifty thousand dollars ($250,000) 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 September 29, 2016, 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 hundred fifty thousand dollars ($250,000) 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, Corporate Secretary 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 rarredando@wecc.biz	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

Heather Laws* Manager 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 *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/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and
Deputy General Counsel
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
sonia.mendonca@nerc.net
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council