PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

November 25, 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, FERC Docket No. NP15-_-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 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 the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE agrees and stipulates to the assessed penalty of one hundred fifty thousand dollars ($150,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement

[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 (2014). *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.

Agreement. Accordingly, the violations in this Full Notice of Penalty 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 Settlement Agreement. 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 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
WECC2013012579	CIP-002-2	R3; R3.3	High/ Severe	URE	$150,000
WECC2013012308	CIP-005-3a	R1; R1.5	Medium/ Severe	URE	
WECC2013012582	CIP-007-3a	R7; R7.1	Lower/ Severe	URE	
WECC2013012583	CIP-007-3a	R8; R8.2	Medium/ Severe	URE	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-2 R3; R3.3 (WECC2013012579)

WECC conducted an on-site Compliance Audit of URE (Compliance Audit). The auditors found that URE did not include relays at sites on its Critical Asset list as Critical Cyber Assets (CCAs). The auditors identified these devices as critical because they were classified by URE's CCA identification methodology as essential to the operation of the Critical Asset.

WECC determined that URE had a violation of CIP-002-2 R3 for failing to develop a complete list of CCAs essential to the operation of 11 Critical Assets.

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, the dial-up accessible protective relaying devices that were not identified as CCAs are capable of tripping transmission lines if the dial-up access capability is compromised. URE's failure to identify these devices as CCAs limited the protections afforded to these devices and increased the opportunity for intentional and unintentional misuse to occur. However, URE did apply some compensating measures. The dial-up accessible system was protected by authentication servers and dial-up gateway devices. The authentication servers were designed to prevent unauthorized access, and WECC reviewed the logs to verify that the servers denied unauthorized access.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. disconnect the dial-up remote access to the relays at Critical Asset substations that have energy management systems (EMS);
2. disconnect the dial-up access for relays at one Critical Asset substation which did not possess the equipment to provide EMS fault data reporting capability;
3. configure and connect EMS fault data reporting on the remaining relays identified as in scope for this violation and disconnect dial-up remote access; and
4. update URE's documentation used to determine what computer systems are CCAs to account for the NERC guidance document that clarifies the scope for dial up accessible devices.[4]

URE certified the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

[4] On June 17, 2010, NERC issued a guidance document named *Identifying Critical Cyber Assets (v1.0): Serial Cyber Assets that are Accessible via Dial-Up.* The document clarified NERC and WECC's approach to CIP-002.

CIP-005-3a R1; R1.5 (WECC2013012308)

URE submitted a Self-Report to WECC citing noncompliance with CIP-005-3a R1. URE reported that it failed to afford one of the protective measures specified in CIP-005-3a R1.5 to Cyber Assets used in the access control and monitoring of the ESPs. URE failed to document the assessment of 47 security patches for 38 electronic access control and monitoring devices (EACMs) within 30 days of being released, as specified in CIP-007 R3. Specifically, URE reported that its firewall vendor made 43 security patches available from its website. URE's assessment exceeded the 30 days allowed by CIP-007-3 R3.1 and URE's procedure. Further investigation found that URE's other firewall vendor made four security patches available. URE failed to document the assessment of these patches within 30 days.

WECC determined that URE had a violation of CIP-005-3a R1 for failing to afford one of the protective measures specified in R1.5 to Cyber Assets used in the access control and monitoring of the ESPs.

WECC determined the duration of the violation to be from 31 days following the release of the first set of security patches for EACM devices, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented around-the-clock logging and monitoring of all user access, and network traffic through and to the access points is sent to a centralized system to alert and dispatch personnel as necessary based on the type and level of anomalous activity. This would allow security personnel to block unauthorized access to the access points, thereby preventing compromise of CCAs within the ESP. URE also implemented a host-based intrusion detection system and antivirus tools which reside on most Windows Cyber Assets within the ESPs. This system can detect and prevent any anomalous activity based on malicious code signatures and other security thresholds set to alert appropriate security personnel. Detection of security vulnerabilities being exploited within the ESP was highly likely based on these detective controls. Detection of this type of activity would allow security personnel to disable communication through the access points to CCAs within the ESP, which would disable control from an outside attacker.

Further, if any anomalous activity resulting from exploitation of security vulnerabilities was detected, URE would have likely corrected the condition because URE implemented good corrective controls. Specifically, URE implemented redundancy in the access points protecting the control center ESPs, which would allow the entity to immediately recover if one of the access points failed. Also, URE would know immediately if any failures or suspicious traffic was occurring based on the logging of the access points, which would invoke security incident procedures or recovery procedures based on the

severity of the incident. The security personnel are trained on security incident analysis and how to recover from failures and incidents affecting Cyber Assets.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update a reoccurring task to provide automated email reminders to the Cyber Asset administrator(s);
2. update a reoccurring task to provide automated email reminders to the respective supervisor or manager assigned responsibility for the completion of firewall security patching; and
3. include notification to a department external to the firewall team for additional awareness of approaching deadlines and obligations ensuring task is completed in a compliant manner.

URE certified on that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R7; R7.1 (WECC2013012582)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R7. The audit team reviewed the disposal, redeployment, and media erasure/sanitation logs of randomly selected groups of Cyber Assets for the audit period and discovered five Cyber Assets where URE did not erase data storage media prior to disposal. The devices consisted of one Physical Access Control System (PACS) device and four non-critical Cyber Assets. URE provided evidence showing that one of the five devices had not been disposed of yet. URE was unable to provide evidence that the media was erased prior to disposal of the other four devices.

WECC determined that URE had a violation of CIP-007-3a R7 for failing to destroy or erase data storage media on four Cyber Assets to prevent unauthorized retrieval of sensitive cybersecurity data.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls that included physical security mechanisms with guards, special locks, closed circuit television, and logical perimeters, along with internal cybersecurity controls such as firewalls.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. add an IT security and compliance review to its change management procedures;
2. update its current checklist for hardware disposal;
3. add a peer review to the disposal and redeployment procedures;
4. create an inventory checklist destruction bin;
5. add a close-out peer review to the change management procedures; and
6. provide peer reviewer training.

URE certified that the above Mitigation Plan requirements were completed.

WECC verified that URE's Mitigation Plan was complete.

CIP-007-3a R8; R8.2 (WECC2013012583)

During the Compliance Audit, WECC discovered that URE had a violation of CIP-007-3a R8. Based on a review of URE's Cyber Vulnerability Assessment (CVA) procedures document, it appeared that the annotated tasks to perform a CVA review of Cyber Assets were "freeform and optional." URE's procedures allowed a vulnerability assessor to perform a subjective review of enabled ports and services on a subset of identified Cyber Assets. It also gave a vulnerability assessor the option to perform a subjective review of hardening statement, which equates to a subject matter expert reviewing a hardening document for a Cyber Asset to determine if the hardened configuration supports the required open ports and services. The assessor is also given the option to review the access control lists of access control systems to assess whether traffic restrictions are too lenient. None of the optional procedures annotated within the CVA procedures document would result in a deliverable that would demonstrate proof of compliance.

WECC determined that URE did not conduct a CVA of ports and services for all Cyber Assets. The scope of the violation includes over CCAs, over 30 non-critical Cyber Assets, over 20 EACMs, and less than 10 PACS devices.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to perform CVAs that included a review to verify that only ports and services required for operation of all Cyber Assets within the ESP are enabled.

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 BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to perform a CVA of Cyber Assets to ensure that only those ports and services required for normal and emergency operations were enabled could have led to a port or service of an associated critical application or system being unknowingly compromised. Such compromise could be used for a debilitating effect on the entity's multiple BES facilities.

However, URE implemented a defense-in-depth architecture of physical and logical cybersecurity controls, including physical security mechanisms with guards, special locks, closed circuit television, and logical perimeters, along with internal cybersecurity controls, including firewalls, vulnerability scanning tools, intrusion detection systems, and a security events management system. Unauthorized access or other malicious use of the potentially vulnerable ports would have been difficult because the devices resided within an ESP and were actively monitored with a high likelihood of being detected upon compromise.

URE's Mitigation Plan to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. tune its vulnerability identification tool for use in the annual CVA process and then run the tool in the production environment;
2. create and validate ports and services baseline with Cyber Assets administrators; and
3. perform updates to the annual CIP CVA procedures to ensure they are more specific and also to include the use of the tool.

URE certified that the above Mitigation Plan requirements were completed.

WECC has not yet verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty thousand dollars ($150,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's violation history as an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE self-reported the violation of CIP-005-3a R1;
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. the violations of CIP-005-3a R1; R1.5 and CIP-007-3a R7; R7.1 posed a minimal risk to the reliability of the BPS, and the violations of CIP-002-2 R3 (R3.3) and CIP-007-3a R8 (R8.2) posed a moderate risk but 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 one hundred fifty thousand dollars ($150,000) 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[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 Settlement Agreement and supporting documentation on November 11, 2014 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.

[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).

In reaching this determination, the NERC BOTCC also considered the factors considered by WECC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty thousand dollars ($150,000) 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.

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) 582-3918 – facsimile jrobb@wecc.biz	Sonia C. Mendonça* Associate General Counsel and Senior 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 Christopher Luras* Director of Compliance Risk Analysis and Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile

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.	

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

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

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

Sonia C. Mendonça
Associate General Counsel and Senior
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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments