PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2013

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. 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 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] of CIP-002-1 R3[4] and CIP-005-3a R2.4. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred forty-four thousand dollars ($144,000), 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. Accordingly, the violations identified as NERC

[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.

[4] This violation was reported as CIP-002-3 through a Self-Certification. However, Version 1 was in effect when the violation began.

Violation Tracking Identification Numbers WECC2013012051, WECC2013012052 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 executed on October 4, 2013, by and between WECC and URE, which is included as Attachment a. 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 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, 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-2218	WECC2013012051	CIP-002-1	R3	High	$144,000
			WECC2013012052	CIP-005-3a	R2.4	Medium	

CIP-002-3 R3

The purpose statement of Reliability Standard CIP-002-3 provides:

> NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and

processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

Standard CIP-002-3 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> > R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
> >
> > R3.2. The Cyber Asset uses a routable protocol within a control center; or,
> >
> > R3.3. The Cyber Asset is dial-up accessible.

CIP-002-3 R3 has a "High" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE submitted a Self-Certification, stating that it had failed to classify devices as Critical Cyber Assets (CCAs) that used a routable protocol to communicate outside the Electronic Security Perimeter (ESP) and were essential for the operation of its Critical Assets. At one time, these devices had been disconnected from URE's corporate environment and had been reconnected to the corporate environment without being properly tracked.

WECC determined that URE was in violation of CIP-002-1 R3 because URE failed to identify devices as CCAs. The devices at issue should have been identified as essential to the operation of a Critical Asset under URE's essentiality definition.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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 identify devices as CCAs limited the protections afforded to these devices and increased the opportunity for intentional or unintentional attacks to occur. The devices were located across Critical Assets in different locations. The devices were not located within a Physical Security Perimeter (PSP) and were not afforded protections associated with PSPs and the protections required by CIP-003 through CIP-009. URE's failure was a result of insufficient procedures for identifying devices as CCAs. URE did not properly track its devices and was unaware that the devices in scope had been disconnected and then reconnected to its corporate environment without being properly tracked. However, the risk was mitigated by several factors. All of the devices were only remotely accessible from URE's corporate network. URE owns all communication channels, and therefore does not use the internet or public wires. In addition, all of the devices were secured within substation control houses where physical access is restricted.

CIP-005-3a R2.4

The purpose statement of Reliability Standard CIP-005-3a R2.4 provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a R2.4 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

CIP-005-3a R2.4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Certification addressing a violation of CIP-005-3a R2. Specifically, URE reported that users on devices within URE's Energy Management System (EMS) ESP could use secure shell, virtual network computing, or remote desktop to obtain a remote login to devices within URE's Generation Management System (GMS) ESP. URE reported that this remote login only required a user name and password to authenticate.

WECC determined that URE was in violation of CIP-005-3a R2 because URE failed to implement strong procedural or technical controls at certain access points to its ESP. URE's EMS ESP had interactive access to URE's GMS ESP. URE was required to have strong technical or procedural controls to ensure authenticity of the accessing party, but the use of usernames and passwords to authenticate the accessing party did not qualify as strong technical or procedural controls.

WECC determined the duration of the violation to be when URE identified the access points as CCAs, through the present.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did not have full assurance of the identity of the individuals with external interactive access to the GMS ESP. However, the risk was mitigated by several factors. All devices involved in the violation were located within a PSP and were protected from unauthorized access through the use of URE's physical access control system. URE actively monitors all remote access and logs any attempts made to access the devices at issue. URE only allows external interactive access to the GMS ESP through the EMS ESP, and both are controlled and restricted ESP networks.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred forty four thousand dollars ($144,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE had two prior violations of CIP-002 R3, which were considered aggravating factors in the penalty determination;

2. URE had an internal compliance program (ICP), which was considered a mitigating factor in the penalty determination;[5]
3. URE completed all of WECC's compliance directives;
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 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 forty-four thousand dollars ($144,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-002-1 R3
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC. The Mitigation Plan was accepted by and approved by. The Mitigation Plan for this violation is designated as WECCMIT009793 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the existing version of its CIP-002 R3 CCA identification policy;
2. create a standard and associated standard operating procedure for connection, disconnection, reconnection of Cyber Assets; and

[5] WECC reviewed URE's ICP and determined that: URE's ICP is documented; the ICP is disseminated throughout its operations staff; URE has ICP oversight staff, which is supervised at a high level in the organization; the ICP oversight staff has independent access to the CEO and the board of directors; URE operates the ICP such that it is independent of staff responsible for compliance with the NERC Reliability Standards; URE has allocated sufficient resources to its ICP; the ICP has the support and participation of senior management; URE reviews and modifies its ICP regularly; URE's ICP includes formal, internal self-auditing for compliance with all Reliability Standards on a periodic basis; and URE's ICP includes disciplinary action for employees involved in violations of the Reliability Standards, when applicable.
[6] *See* 18 C.F.R § 39.7(d)(7).

3. improve training of Subject Matter Experts and other relevant personnel on CCA identification.

URE certified that the above Mitigation Plan requirements were completed. URE submitted evidence of completion of its plan.

CIP-005-3a R2.4

URE's Mitigation Plan to address its violation of CIP-005-3a R2.4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT009812 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. redesign the network security architecture of the EMS and GMS ESPs;
2. create a virtual private network tunnel between the two systems;
3. perform security testing on any new hardware or software required by the redesigned network architecture;
4. update all relevant CIP documentation; and
5. conduct training with all interactive users.

WECC will verify completion of this Mitigation Plan once URE submits a Certification of Mitigation Plan Completion.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

forty-four thousand dollar ($144,000) financial penalty against WECC and other actions to facilitate future compliance required under the terms and conditions of 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.

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

1. URE had two prior violations of CIP-002 R3, which were considered aggravating factors in the penalty determination, as discussed above;
2. URE had an ICP, which was considered a mitigating factor in the penalty determination, as discussed above;
3. URE completed all of WECC's compliance directives;
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 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred forty four thousand dollars ($144,000) 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.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information

related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

The attachments to be included as part of this Notice of Penalty are the following documents:

a) Settlement Agreement by and between WECC and URE, included as Attachment a;

b) URE's Self-Certification for CIP-002-1 R3 and CIP-005-3a R2, included as Attachment b;

c) URE's Mitigation Plan for CIP-002-1 R3, included as Attachment c;

d) URE's Mitigation Plan for CIP-005-3a R2, included as Attachment d; and

e) URE's Certification of Mitigation Plan Completion for CIP-002-1 R3, included as Attachment e.

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