July 31, 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. 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# NCRXXXXXX, 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 neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred eighty thousand dollars ($180,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the

[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.

terms and conditions of the Settlement 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, 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 (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*	Total Penalty
WECC2013011904	CIP-004-1	R3	Medium/ Severe	$180,000
WECC2013012378	CIP-005-1	R1; R1.5	Medium/ Severe	
WECC2013012379	CIP-005-1	R2; R2.4; R2.5	Medium/ Severe	
WECC2013012437	CIP-006-1	R1; R1.8	Medium/ Severe	
WECC2013012381	CIP-007-1	R2	Medium/ Severe	
WECC2013011811	CIP-007-1	R5; R5.2.3	Medium/ Severe	
WECC2013012380	CIP-007-3a	R8	Lower/ Severe	

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

<u>CIP-004-1 R3 (WECC2013011904)</u>

URE submitted a Self-Report to WECC. URE reported that five employees were granted physical access to a Physical Security Perimeter (PSP) without a valid personnel risk assessment (PRA). In addition, URE granted one employee unescorted physical access to a PSP prior to having completed a PRA.

WECC determined that URE failed to ensure PRAs were conducted for six employees prior to granting them physical access to a PSP containing Critical Cyber Assets (CCAs).

WECC determined the duration of the violation to be from thirty days after access was granted for five of the six employees at issue, through when URE revoked access for those five employees, and from when unescorted physical access was granted to the sixth employee, through when URE revoked access.

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 violation exposed the seven CCAs to the possibility of unauthorized access attempts. The risk was not serious or substantial because the CCAs were equipped with electronic access, logging, and monitoring controls. In addition, URE's PSP is monitored 24 hours a day, seven days a week to prevent unauthorized physical access to areas or systems. Five of the six employees in scope had NERC CIP training completed, and all six employees are still employed with URE in good standing. The subsequent PRAs for the five employees revealed no adverse findings and the sixth employee did not access a URE PSP during the six days of access to the PSP.

URE's Mitigation Plan (WECCMIT009626) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. implement a new PRA process; and
2. enhance its access controls by implementing a procedure which no longer allows dual approval rights for physical or cyber access.

URE certified that the above Mitigation Plan requirements were completed. WECC verified that URE's Mitigation Plan was complete.

<u>CIP-005-1 R1.5 (WECC2013012378)</u>

WECC performed a Compliance Audit of URE. WECC determined that URE failed to ensure two Cyber Assets used in the electronic access control and monitoring of Electronic Security Perimeters (ESPs) were afforded the protective measures of CIP-003, CIP-004 R3, CIP-005 R2 and R3, CIP-006 R2 and R3, CIP-007 R1 and R3 through R9, CIP-008, and CIP-009. Specifically, the devices at issue consisted of a firewall manager and server.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through the present.

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, failing to provide Cyber Assets the required protective measures puts such assets and ESPs at risk to be manipulated or compromised. Such information could then be used to get access to CCAs essential to the operation of the BPS and thereby potentially disrupt the operation of the BPS. The risk was not serious or substantial because the ESPs were equipped with a security incident and events management (SIEM) technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. Finally, there was no actual manipulation or compromise of the Cyber Assets at issue or the CCAs essential to the operation of the BPS.

URE's Mitigation Plan (WECCMIT010576) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. implement CIP-005 controls on the firewall manager; and
2. deploy the physical infrastructure required for a password vault.[4]

<u>CIP-005-1 R2: R2.4 and R2.5 (WECC2013012379)</u>

WECC performed a Compliance Audit of URE. WECC reviewed URE's processes and procedures associated with electronic access controls, and examined the configurations of all access points to the ESPs. WECC determined that URE failed to implement strong procedural or technical controls of electronic access at all access points to the ESPs. Specifically, URE's documentation failed to identify and describe the process for access requests and authorization for external interactive access into the ESP. In addition, URE's required documentation failed to identify and describe the authentication methods.

[4] The password vault manages shared accounts. Each shared account is assigned a policy and a vault. The policy sets the rules that facilitate shared password management and controls how often the password should be changed and who has access to the account. The vault is a logical container for storing passwords. Access to vaults is restricted based on who will need access to the shared accounts and passwords stored within the vaults. Accessing the vaults and the shared accounts in the vault creates the unique audit trial.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through present.

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, failing to implement and document technical and procedural controls of electronic access at all electric access points to ESPs puts such assets and ESPs at risk to be manipulated or compromised. The risk was mitigated because the ESPs were equipped with an SIEM technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. There was no manipulation or compromise of the assets within the ESPs, the ESPs themselves, or the access points.

URE's Mitigation Plan (WECCMIT010577) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. conduct a planning and coordination meeting related to URE two-factor authentication in the generation management system (GMS); and
2. deploy the physical infrastructure required for two-factor authentication.

<u>CIP-006-1 R1.8 (WECC2013012437)</u>

WECC performed a Compliance Audit of URE. WECC conducted site visits to visually observe and verify that all PACS are protected from unauthorized physical access. WECC determined that URE failed to provide protective measures specified in R1.8 to Cyber Assets that authorize and/ or log access to PSPs. The devices in scope are seven workstations, one server, and six door controllers that manage, log, monitor, and provision access to all of URE's PSPs. Further, URE failed to file Technical Feasibility Exceptions (TFEs) for the six door controllers that could not technically support security logging.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through present.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PACS devices were physically located within a protected facility with physical and electronic monitoring and alarming at all times. The workstations and server reside behind the corporate firewall configured to restrict, monitor, and alert upon suspected malicious activity. The six door controllers did not have the technical capability to log security events or the ability to grant unintentional access to individuals with malicious intent. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010577) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. submit TFEs for six door controllers;
2. evaluate and develop an architectural design to ensure strong authentication for external interactive access for the PACS;
3. conduct a status meeting to ensure the project deliverables are on target; and
4. implement strong technical controls for external interactive access to the PACS by requiring the seven administrator workstations to access the PACS via Windows terminal servers for two-factor authentication.

CIP-007-1 R2 (WECC2013012381)

WECC performed a Compliance Audit of URE. WECC determined that for three years URE failed to enable only those ports and services required for normal and emergency operations for 21 CCAs, 2 non-CCAs, 8 Electronic Access Control and Monitoring Devices (EACMs), and 7 PACS assets. Further, URE failed to establish a process to ensure that only those ports and services required for normal and emergency operations 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, the devices in scope (networking equipment) are used to support 100% of URE's ESPs. The risk was mitigated because the ESPs were equipped with an SIEM technology that provides security information and events management on all URE ESPs. Traffic to and from URE's ESPs must first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards, cameras, and special locks. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010329) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. document the baseline ports and services in compliance with CIP-007; and
2. update its procedures to ensure the baseline documents are reviewed on an annual basis.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R5.2.3 (WECC2013011811)

URE submitted a Self-Report to WECC. URE stated it did not have a policy for managing the use of some of its shared accounts. URE has controls in place for managing who has access to the accounts, but no process in place to determine who was using the shared accounts at any given time. WECC determined that URE failed to create an audit trail of the shared accounts. The devices in scope include workstations, servers, EACMs, PACS, and access points.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through present.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE has implemented account controls on all shared accounts. Specifically, URE personnel require domain level usernames and passwords in order to access the shared accounts and all shared accounts are equipped with 24 hour a day, seven day a week monitoring and logging. The URE personnel that have access to the shared accounts in scope have PRAs and CIP training. All the devices that use the shared accounts are located within a PSP where physical access is restricted by guards and special locks. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010721) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. use the vault to meet the requirements of Standard CIP-007 R5;
2. conduct a planning and coordination meeting to discuss build-out and design of the vault technology;
3. deploy the physical infrastructure required for the vault;
4. configure the network infrastructure required for the vault; and
5. test and deploy the vault and update related documentation.

CIP-007-3a R8 (WECC2013012380)

WECC performed a Compliance Audit of URE. WECC determined that URE failed to conduct an annual Cyber Vulnerability Assessment (CVA) on all Cyber Assets within an ESP. Specifically, during the calendar year, URE failed to conduct a CVA on six assets. The assets included four CCAs (GMS workstations) and two PACS devices.

WECC determined the duration of the violation to be from when URE failed to conduct its CVA, 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. The assets at issue were located within a single ESP that is equipped with intrusion detection systems and an SIEM technology that provides security information and events management. Traffic to and from URE's ESPs but first pass through firewalls configured to restrict, monitor, and alert upon suspected malicious activity. The devices in scope are located in physically secure areas where physical access is restricted by guards and special locks. URE did perform a CVA on the remaining Cyber Assets within the GMS domain. In addition, this violation resulted in no actual harm to the BPS.

URE's Mitigation Plan (WECCMIT010330) to address this violation was submitted to WECC.

URE's Mitigation Plan required URE to:

1. update the CVA procedure to ensure the assessment includes a comparison of baseline ports and services to then-running ports and services for all Cyber Assets and documenting any discrepancies for remediation; and
2. conduct a CVA on all Cyber Assets pursuant to Standard CIP-007 R8.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred eighty thousand dollars ($180,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered URE's compliance history as an aggravating factor in the penalty determination;

2. URE had an internal compliance program (ICP) at the time of the violation, which WECC considered a mitigating factor;
3. URE self-reported the violation of CIP-004-1 R3, which WECC considered a mitigating factor in penalty determination;[5]
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-006 R1, CIP-007 R5, and CIP-007 R8 posed a minimal risk but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above. The violations of CIP-004 R3, CIP-005 R1, CIP-005 R2, and CIP-007 R2 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 eighty thousand dollars ($180,000) 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[6]

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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 15, 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

---

[5] Although URE also self-reported the violation of CIP-007-1 R5, URE submitted the Self-Report during the Self-Certification period, and therefore WECC did not apply self-reporting credit for that violation.

[6] *See* 18 C.F.R. § 39.7(d)(4).

[7] *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).

underlying facts and circumstances of the violations at issue. In reaching this determination, the NERC BOTCC also considered the factors above that WECC considered.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) 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.

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 801-883-6853 (801) 582-3918 – facsimile jrobb@wecc.biz	Sonia C. Mendonça* Associate 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* 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 Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (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 Chris 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 CLuras@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,

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

/s/ Edwin G. Kichline
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 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