

December 29, 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 Penalty¹ 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 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 28 violations³ of Critical Infrastructure Protection (CIP) Reliability Standards.

According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

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.

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 2

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	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902111	CIP-002-1	R1	Medium/ Severe	GO, GOP	SR	Minimal	No Penalty
WECC200902115	CIP-002-1	R3	High/ Severe		SR	Moderate	
WECC200902116	CIP-002-1	R4	Lower/ Severe		SR	Minimal	
WECC200902133	CIP-004-1	R2	Medium/ Severe		SR	Moderate	
WECC200902130	CIP-004-1	R4	Medium/ Severe		SR	Moderate	
WECC200902120	CIP-005-1	R1	Medium/ Severe		SR	Moderate	
WECC200902121	CIP-005-1	R2	Medium/ Severe		SR	Moderate	
WECC200902124	CIP-005-1	R4	Medium/ Severe		SR	Moderate	

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 3

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902132	CIP-005-1	R5	Lower/ Severe	GO, GOP	SR	Minimal	No Penalty
WECC2013012269	CIP-005-3a	R3	Medium/ Severe		CA	Moderate	
WECC200902289	CIP-006-1	R1	Medium/ Severe		SR	Moderate	
WECC200902129	CIP-006-1	R2	Medium/ Severe		SR	Minimal	
WECC200902128	CIP-006-1	R3	Medium/ Severe		SR	Minimal	
WECC200902125	CIP-006-1	R4	Lower/ Severe		SR	Minimal	
WECC200902136	CIP-006-1	R6	Medium/ Severe		SR	Moderate	
WECC2013011735	CIP-006-3c	R2	Medium/ Severe		SR	Minimal	
WECC2013011732	CIP-006-3c	R4	Medium/ Severe		SR	Minimal	
WECC2013011733	CIP-006-3c	R5	Medium/ Severe		SR	Minimal	
WECC2013011734	CIP-006-3c	R6	Lower/ Severe		SR	Minimal	
WECC200902137	CIP-007-1	R1	Medium/ Severe		SR	Minimal	
WECC200902127	CIP-007-1	R2	Medium/ Severe		SR	Moderate	

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 4

NERC Violation ID	Standard	Req	VRF/ VSL	Applicable Function(s)	Discovery Method*	Risk	Penalty Amount
WECC200902126	CIP-007-1	R3	Lower/ Severe	GO, GOP	SR	Moderate	No Penalty
WECC200902140	CIP-007-1	R4	Medium/ Severe		SR	Moderate	
WECC200902141	CIP-007-1	R5	Medium/ Severe		SR	Moderate	
WECC200902146	CIP-007-1	R6	Medium/ Severe		SR	Minimal	
WECC200902148	CIP-007-1	R8	Medium/ Severe		SR	Moderate	
WECC200902149	CIP-007-1	R9	Lower/ Severe		SR	Minimal	
WECC2015015259	CIP-007-3a	R6	Medium/ Severe		SR	Minimal	

Common Risk Statement for all Violations

WECC determined the risk that each violation posed to the reliability of the bulk power system (BPS) as shown in the chart above. Although URE had not implemented all processes to become compliant with the requirements of the CIP Reliability Standards, WECC confirmed that URE was following government-issued guidelines that mitigated URE’s risk.

Common Duration for 22 Violations

WECC determined the duration of 22 of the violations to be from the date when each Reliability Standard became mandatory and enforceable on URE, through when URE completed its associated Mitigation Plan.⁴ The approximate durations of the violations was between two and five years.

⁴ WECC200902111, WECC200902115, WECC200902116, WECC200902120, WECC200902121, WECC200902124, WECC200902125, WECC200902126, WECC200902127, WECC200902128, WECC200902129, WECC200902130, WECC200902132, WECC200902133, WECC200902136, WECC200902137, WECC200902140, WECC200902141, WECC200902146, WECC200902148, WECC200902149, and WECC20090228.

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 5

Common Certification and Verification Information for all Violations

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

WECC200902111, WECC200902115, WECC200902116 CIP-002-1 R1, R3, and R4 - OVERVIEW

WECC determined that URE failed to: (1) identify and document a risk-based assessment methodology (RBAM) to identify its Critical Assets; (2) develop a list of associated Critical Cyber Assets (CCAs) essential to the operation of the Critical Asset; and (3) approve annually the list of Critical Assets and the list of CCAs.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Conduct an engineering assessment to determine whether it possesses Cyber Assets essential to the operation of its Critical Assets;
2. Revise its RBAM and its CCA identification methodology to reflect the results of the engineering assessment; and
3. Revise and submit a list of CCAs to reflect the revised RBAM.

WECC200902133 and WECC200902130 CIP-004-1 R2 and R4 - OVERVIEW

WECC determined that URE failed to: (1) establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to CCAs, and review the program annually and update as necessary; and (2) maintain lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to develop procedures establishing a training program for personnel with access to CCAs.

WECC200902120, WECC200902121, WECC200902124, and WECC200902132 CIP-005-1 R1, R2, R4, and R5 - OVERVIEW

WECC determined that URE failed to: (1) ensure that every CCA resided within an Electronic Security Perimeter (ESP), and identify and document the ESP and all access points to the perimeters; (2) implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all Electronic Access Points to the ESP; (3) perform a Cyber Vulnerability

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 6

Assessment (CVA) of the Electronic Access Points to the ESP at least annually; and (4) review, update, and maintain all documentation to support compliance with the requirements of the Reliability Standard.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Ensure that every CCA resides within an ESP and document it on drawings;
2. Implement and document the organizational processes and procedural mechanisms for control of electronic access at all points of the ESP;
3. Perform and document a CVA of the electronic access points to the ESP annually; and
4. Review, update, and maintain all documentation to support compliance with the requirements of the Reliability Standard.

WECC2013012269 CIP-005-3a R3 - OVERVIEW

WECC determined that URE failed to implement and document electronic or manual processes for monitoring and logging access at ESP access points.

WECC determined the duration of the violation to be approximately 10 months, from the date when URE failed to implement and document electronic or manual processes for monitoring and logging access at all ESP access points, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to develop, test, send, and install new software configurations at both of the facilities within scope.

WECC200902289, WECC200902129, WECC200902128, WECC200902125, and WECC200902136 CIP-006-1 R1, R2, R3, R4, and R6 - OVERVIEW

WECC determined that URE failed to: (1) document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter (PSP) 24 hours a day, seven days a week; (2) document and implement operational and procedural controls to manage physical access at all access points to the PSP 24 hours a day, seven days a week; (3) document and implement the technical and procedural controls for monitoring physical access at all access points to the PSP 24 hours a day, seven days a week; (4) log with sufficient information to identify individuals uniquely and the time of access 24 hours a day, seven days a week, and implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSP using

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 7

computer logging, video recording, or manual logging; and (5) implement a maintenance and testing program to ensure that all required physical security systems function properly.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Develop supporting documentation;
2. Accomplish adequate reviews;
3. Purchase and install communications and security hardware;
4. Install alarms at PSP access points; and
5. Configure security software.

WECC2013011735 CIP-006-3c R2 - OVERVIEW

WECC determined that URE failed to provide three of the protections required by the Reliability Standard to seven Physical Access Control System (PACS) devices. Specifically, WECC determined that URE did not have an auditable trail of use of all shared accounts for the seven PACS devices and also failed to change the password on one shared account after personnel changes. WECC also determined that URE failed to have a password of sufficient complexity for the system administration shared account. Finally, WECC determined URE's CVA for the seven PACS devices did not include a review of ports and services, a review of default accounts, or an action plan to remediate or mitigate vulnerabilities identified in the assessment as required.

WECC determined the duration of the violation to be 3 years and 7 months, from the date when URE failed to provide all required protections to seven PACS devices, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Complete ports and service analysis on the test platform;
2. Investigate ports and services on PACS system;
3. Update and complete CVA on PACS system;
4. Disable unnecessary services on PACS system;

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 8

5. Identify all shared accounts and issue individual user accounts to personnel who do not need to use shared accounts to ensure continuity of operations;
6. Study the feasibility of having its security contractor use individual user accounts rather than shared user accounts;
7. Remove shared administrator accounts, except where it is not technically feasible to use individual administrator accounts;
8. Implement a policy or procedure to ensure that shared account passwords are changed any time a shared account user leaves the organization;
9. Implement regularly scheduled password changes;
10. Provide additional training on the requirements of CIP Reliability Standards to the employees responsible for the system administration of PACS, along with their first- and second-line supervisors. Further, provide training on the importance of the CVA to cyber security and the necessity of effective and accurate communication to URE's culture of compliance; and
11. Change the PACS password to ensure that it meets the minimum complexity requirements.

WECC2013011732 CIP-006-3c R4 - OVERVIEW

WECC determined that URE failed to implement the operational and procedural controls to manage physical access to two PSPs 24 hours a day, seven days a week.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the operational and procedural controls, through when URE implemented the proper methods to control physical access to the two PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Immediately secure the control room and cable spreading room doors;
2. Install restricted key lock cores on the control room and cable spreading room doors; and
3. Restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 9

WECC2013011733 CIP-006-3c R5 - OVERVIEW

WECC determined that URE failed to implement the technical and procedural controls for monitoring physical access at three access points as required.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the technical and procedural controls for monitoring physical access to three access points to the PSPs, through when URE implemented the proper methods to monitor physical access to the PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to:

1. Immediately secure the control room and cable spreading room doors;
2. Install restricted key lock cores on the control room and cable spreading room doors; and
3. Restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

WECC2013011734 CIP-006-3c R6 - OVERVIEW

WECC determined that URE failed to implement the technical and procedural controls for logging physical access at three access points as required.

WECC determined the duration of the violation to be approximately one week, from the date when URE failed to implement the technical and procedural controls for monitoring physical access to three access points to the PSPs, through when URE implemented the proper methods to control physical access to the PSPs.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to restore the PACS, which actively controls, logs, and monitors physical access points to the PSP, to operation.

WECC200902137, WECC200902127, and WECC200902126, CIP-007-1 R1, R2, and R3 - OVERVIEW

WECC determined that URE failed to: (1) ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls; (2) establish, document, and implement a process to ensure that it only enabled those ports and services required for normal and emergency operations; and (3) establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESP.

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 10

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Perform a CVA on the supervisory control and data acquisition (SCADA) system;
2. Complete investigation of ports and services on the generic data acquisition and control system (GDACS) system;
3. Disable unnecessary ports and services on the SCADA system, where possible, and update the system baseline to include all ports and services;
4. Complete full port scans;
5. Ensure that, for GDACS Cyber Assets within an ESP, it enabled only ports and services required for normal and emergency operations, and disabled all other ports and services; and
6. Assess security patches.

WECC200902140, WECC200902141, WECC200902146, WECC200902148, and WECC200902149 CIP-007-1 R4, R5, R6, R8, and R9 - OVERVIEW

WECC determined that URE failed to: (1) use anti-virus software and other malicious software or malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP; (2) establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access; (3) ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor cyber security system events; (4) perform a CVA of all Cyber Assets within the ESP at least annually as required; and (5) review and update the documentation specified in the Reliability Standard at least annually.

URE submitted its Mitigation Plan to address the referenced violations, which required URE to:

1. Perform a new CVA with an updated execution status;
2. Complete investigation of ports and services on the GDACS system;
3. Disable unnecessary ports and services on the SCADA system, where possible, and update the system baseline to include all ports and services;

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 11

4. File Technical Feasibility Exceptions for all remaining GDACS devices that are not capable of enforcing strong passwords;
5. Adopt a standard form for tracking shared account use;
6. Complete disabling unused ports and services identified;
7. Complete disabling all default accounts identified;
8. Complete CVA for all GDACS Cyber Assets within an ESP; and
9. Formally document default account review for all GDACS Cyber Assets within an ESP.

WECC2015015259 CIP-007-3a R6 - OVERVIEW

WECC determined that URE failed to ensure all Cyber Assets within the ESP had automated tools or organizational process controls to monitor system events related to cyber security.

WECC determined the duration of the violation to be ten months, from the date when URE upgraded its SCADA computers' operating systems without enabling all required alert alarms, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violation, which required URE to correct the alarming problem, test it on an off-line test platform, and install the correct configuration.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed no penalty 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 disposition method for the violations described in NERC Violation IDs WECC2013011732, WECC2013011733, WECC2013011734, WECC2013011735, and WECC2015015259. WECC determined that URE's compliance history was not relevant for the violations described in NERC Violation IDs WECC200902111, WECC200902115, WECC200902116, WECC200902120, WECC200902121, WECC200902124, WECC200902125, WECC200902126, WECC200902127, WECC200902128, WECC200902129, WECC200902130, WECC200902132, WECC200902133, WECC200902136, WECC200902137, WECC200902140, WECC200902141, WECC200902146, WECC200902148, WECC200902149, WECC200902289, and WECC2013012269;

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 12

2. URE voluntarily self-reported 27 of the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. fourteen violations posed a minimal, and 14 violations posed a moderate, and not a serious or 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 disposition.

After consideration of the above factors, WECC determined that, in this instance, it would issue no penalty.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed⁵

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 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 disposition 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.

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).

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 13

Notices and Communications: Notices and communications with respect to this filing may be addressed to the following:

<p>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</p> <p>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</p> <p>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</p>	<p>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</p> <p>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</p>
--	---

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 14

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.

NERC Notice of Penalty
Unidentified Registered Entity
December 29, 2016
Page 15

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

Attachments