November 30, 2015

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. NP16-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) submits this Notice of Penalty[1] regarding Unidentified Registered Entity (URE). This Notice of Penalty provides information and details regarding the nature and resolution of the violations,[2] 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)).[3]

NERC is filing this Notice of Penalty with the Commission because Western Electricity Coordinating Council (WECC) issued a Notice of Confirmed Violation and Proposed Penalty or Sanction (NOCV) to resolve all outstanding issues arising from WECC's determination and findings of the violations of NERC Reliability Standards.

---

[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 (2015). *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] 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.

[3] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

NERC is filing this Notice of Penalty with the Commission based on information from WECC. URE does not contest the violations or the proposed two hundred and five thousand dollar ($205,000) penalty assessment.

Accordingly, NERC is filing the violations in this Notice of Penalty 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 NOCV issued by WECC. This Notice of Penalty and the NOCV provide the details of the findings and basis for the penalty. This Notice of Penalty filing contains the NERC Board of Trustees Compliance Committee's (NERC BOTCC) basis for approval of the NOCV.

In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2015), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the NOCV.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2014013523	CIP-002-3	R3	High/ High	SC	$205,000
WECC2014014131	CIP-005-3a	R1	Medium/ Severe	SR	
WECC2014013524	CIP-005-3a	R2	Medium/ Severe	SC	
WECC2014014129	CIP-005-3a	R4	Medium/ Severe	SR	
WECC2014013525	CIP-007-3a	R1	Medium/ Severe	SC	
WECC2014014130	CIP-007-3a	R8	Medium/ Severe	SR	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Penalty Amount
WECC2014013526	CIP-007-3a	R9	Lower/ High	SC	$205,000

WECC2014013523 CIP-002-3 R3- OVERVIEW

WECC determined that URE failed to identify a communications multiplexer and protective relay as Critical Cyber Assets (CCAs) when it added the devices to its Electronic Security Perimeter (ESP) as required by CIP-002-3 R3.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE failed to identify two devices as CCAs, the two devices were located within Physical Security Perimeters (PSP) and the ESP. Physical and electronic access to the devices was monitored and restricted to authorized personnel who had background checks and training. The devices were located in protected networks with hardened boundary devices that only allowed traffic from specific IP addresses and ports. URE monitored the communications multiplexer and likely would have been alerted to a loss of communication with the substation. URE conducts annual Cyber Vulnerability Assessments (CVAs) that include a step for network device discovery.

WECC determined the duration of the violation to be from when URE technicians connected the two devices to the ESP, through when URE disconnected both devices from the network.

URE submitted its Mitigation Plan designated WECCMIT011129 to address the referenced violations. URE's Mitigation Plan required URE to:

1. unplug the communications multiplexer from the network;
2. remove access to the protective relay from the firewall and unplug the device;
3. create a new Cyber Asset request form to document proper device identification, ESP, connectivity (IP address), device location, and serial number with post-change validation; and
4. provide training to all construction and engineering groups covering CIP requirements as they apply to each group specifically, including the use of the newly developed forms.

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

WECC2014014131 CIP-005-3a R1- OVERVIEW

WECC determined that URE failed to identify six access points to the ESP that included any externally connected communication end point terminating at any device within the ESP as required by CIP-005-3a R1.1. URE also failed to afford Cyber Assets used in the access control and/or monitoring of the ESP the protective measures specified in CIP-005-3a R1.5.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to identify six devices as access points, the devices in scope are protected by a firewall with strong access controls for all traffic entering the ESP from external networks. The access controls include two-factor authentication. As a result, individuals require username and passwords and a token in order to access URE's network. URE's architecture requires all traffic entering into the separate virtual local area networks (VLANs) connected to the devices first to pass through the firewall and meet the explicit rules on the access point. These measures reduce the risk of successful VLAN hopping necessary to gain unauthorized access using the six devices in scope.

URE also implemented an intrusion prevention system (IPS) over the energy management system (EMS). The EMS IPS scans EMS traffic for known attack signatures and prevents any known attack signatures that are found. The IPS is designed to identify malware used to compromise the EMS supervisory control and data acquisition (SCADA) devices. URE also implemented an intrusion detection system (IDS) for the EMS and other ESPs on the network. The IDS scans traffic on the ESPs and was designed to detect a breach of the network.

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

URE submitted its Mitigation Plan designated WECCMIT011659 to address the referenced violations. URE's Mitigation Plan required URE to:

1. document the configuration of the open ports and services on the three electronic access control and monitoring (EACM) devices;
2. fix the script and modify procedures to verify passwords were successfully changed after the script is run;
3. manually change passwords for all six devices in scope;
4. train all information technology security staff members on new procedure;
5. fix internal process to verify script is working;

6. modify CVA processes and procedures to ensure all steps were completed correctly by all groups; and
7. provide training to all personnel involved in performing CVAs as well as those responsible for reviewing CVA results.

WECC2014013524 CIP-005-3a R2- OVERVIEW

WECC determined that URE failed to use an access control model where explicit permissions were specified, and failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP as required by CIP-005-3a R2.1 and R2.2.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to use an access control model where explicit permissions were specified and failed to enable only required ports and services, URE implemented restrictive boundary security controls that had a limited set of IP addresses and services in scope. This control limited the unnecessary vectors a malicious user could attempt to use. URE also implemented strong username and passwords, malicious software prevention tools, and logical monitoring of event logs and access attempts. This control reduced the likelihood that a malicious user could gain access to devices once inside the ESP. URE also implemented alerts on the remote terminal units (RTUs). This control would likely notify URE's control center personnel if a device's connection were lost. Finally, URE also conducted annual CVAs to verify the posture of devices.

WECC determined the duration of the violation to be from when URE put its new EMS into production and did not ensure an unnecessary service was disabled at one ESP access point, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011128 to address the referenced violations. URE's Mitigation Plan required URE to:

1. correct the firewall rules to prevent unauthorized access;
2. complete a full review of existing profiles of business areas for ports and services to determine that ports are accurately and clearly documented; and
3. make additional improvements to the process and training of personnel that will be included in the CIP Version 5 implementation plan.

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

WECC2014014129 CIP-005-3a R4- OVERVIEW

WECC determined that for two calendar years, URE failed to include a review during its Cyber Vulnerability Assessment (CVA) to ensure it had enabled only ports and services necessary for operations at the access points and URE failed to document the ports and services in the CVA results and action plan as required by CIP-005 R4.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE implemented preventive controls to address vulnerabilities. These preventive controls included an IPS to scan for and block known attack packet signatures. URE also implemented an antivirus designed to identify and stop malware in the attack packet. The second layer of URE's EMS, the switches, does not support the same port the firewall rule enabled. As a result, the switches would not allow a potential attack to move from the firewalls to the SCADA devices using the port enabled by the firewall rule. URE also implemented detective controls. URE implemented IDS to scan the system for known attack signatures. URE also uses a security information and event management to detect malicious activity and alert appropriate personnel of malicious activity.

WECC determined the duration of the violation to be from when URE first failed to verify in its CVAs that only open ports and services required for operations were enabled, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011445 to address the referenced violations. URE's Mitigation Plan required URE to:

1. modify the existing access point rules to correct the identified issues; and
2. complete the CVA for the EMS and substation access points in order to validate corrections were made.

WECC2014013525 CIP-007-3a R1- OVERVIEW

WECC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls as required by CIP-007-3a R1.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS.

Although URE failed to test firmware upgrades applied to its devices and failed to test additional devices prior to installation, all of the devices were located within PSP. URE limited physical access to

appropriately authorized personnel. All of the devices were installed in an ESP, and URE limited logical access to appropriately authorized personnel. The devices were logically protected by an access point that restricts ports and services. The ESP also logged and monitored malicious activity and likely would have detected abnormal activity on the devices. The relays in scope were located in protected networks with hardened boundary devices and only allowed traffic from specific IP addresses and ports. URE implemented alerts on the RTUs in scope that likely would have notified URE personnel if a link were broken or lost. URE conducted annual CVAs to verify the security posture of the devices in scope. URE also implemented a process to review previous changes made and verify testing was conducted on those changes.

WECC determined the duration of the violation to be from when URE upgraded firmware on devices within the ESP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011127 to address the referenced violations. URE's Mitigation Plan required URE to:

1. compile the devices and associated information in a single list that includes the name of the device (and previous name which will be found in evidence if the name of the device changed), device class, critical asset, IP address, and Technical Feasibility Exceptions;
2. confirm that the upgrade did not change the existing configuration information for the devices beyond version information;
3. perform the validation as part of the CVA; and
4. provide evidence of the validation of the shared accounts and password settings.

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

WECC2014014130 CIP-007-3a R8- OVERVIEW

WECC determined that URE failed to perform a CVA of all Cyber Assets within the ESP during two calendar years as required by CIP-007-3a R8.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE failed to perform a CVA for the eight switches, URE did implement preventive and compensating controls. URE implemented an IPS designed to scan network traffic for known attack signatures and discover and block malware attacks on the switches. URE also implemented an IDS designed to scan network traffic for known attack patterns and signatures and detect an attacker intruding on the system. URE deployed an antivirus to scan and block attack signatures and malware.

In addition, URE also implemented defense in depth with multiple firewalls between the switches in scope and the border of the network. The defense in depth would require a potential attacker to bypass all layers of the firewall in order to attempt to exploit the switches. URE also used two-factor authentication on its EMS devices, reducing the likelihood of a potential attacker comprising a device.

WECC determined the duration of the violation to be from when URE first failed to perform the CVA of all Cyber Assets within the ESP, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011294 to address the referenced violations. URE's Mitigation Plan required URE to perform a CVA on the EMS network switches.

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

WECC2014013526 CIP-007-3a R9- OVERVIEW

WECC determined that URE failed to ensure that changes resulting from modifications to the systems or controls were documented within 30 calendar days of the change being completed as required by CIP-007-3a R9.

WECC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS.

Although URE failed to provide complete test results within 30 calendar days of when the devices were connected to the ESPs, all of the devices were located within PSPs. URE limited physical access to appropriately authorized personnel. All of the devices were installed in an ESP, and URE limited logical access to appropriately authorized personnel. The devices were logically protected by an access point that restricts ports and services. The ESP also logged and monitored malicious activity and likely would have detected abnormal activity on the devices. The relays in scope were located in protected networks with hardened boundary devices and only allowed traffic from specific IP addresses and ports. URE implemented alerts on the RTUs in scope that likely would have notified URE personnel if a link were broken or lost. URE conducted annual CVAs to verify the security posture of the devices in scope. URE also implemented a process to review previous changes made and verify testing was conducted on those changes.

WECC determined the duration of the violation to be from 31 calendar days after URE first made changes resulting from modifications to the systems or controls, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan designated WECCMIT011295 to address the referenced violations. URE's Mitigation Plan required URE to perform a CVA and use the results to confirm that the baseline configurations were correct and unchanged.

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

Regional Entity's Basis for Penalty

According to the NOCV, WECC has assessed a penalty of two hundred and five thousand dollars ($205,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC considered the instant violations as repeat noncompliance of NERC Reliability Standards and determined the compliance history should serve as an aggravating factor;
2. URE had an internal compliance program at the time of the violation which WECC considered a mitigating factor;
3. URE did not receive mitigating credit for self-reporting because the Self-Reports were submitted after receiving notice of an upcoming Compliance Audit;
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 WECC2014013523, WECC2014014131, WECC2014013524, WECC2014014129, and WECC2014014130 posed a minimal and not serious or substantial risk to the reliability of the BPS. The violations of WECC2014013525 and WECC2014013526 posed a moderate and not serious or substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that the penalty amount of two hundred and five thousand dollars ($205,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the NOCV and supporting documentation on November 3, 2015 and approved the NOCV. In approving the NOCV, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

The NERC BOTCC approved the NOCV and believes that the assessed penalty of two hundred and five thousand dollars ($205,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

Pursuant to 18 C.F.R. § 39.7(e), the penalty will be effective upon expiration of the 30-day period following the filing of this Notice of Penalty with FERC, or, if FERC decides to review the penalty, upon final determination by FERC.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Michael Moon* Vice President Entity Oversight Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7608 (801) 883-6894 – facsimile mmoon@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net *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
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

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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council