PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

April 30, 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 (URE), 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), 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-005-1 R1, CIP-005-3 R4, CIP-007-1 R1, R3, and R6, CIP-007-2a R4, and CIP-007-3a R2, R5, and R8. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty-five thousand dollars ($155,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of 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 (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.

Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC2012010739, WECC2012010740, WECC2012011029, WECC2012010439, WECC2012011031, WECC2012011329, WECC2012011032, WECC2012011034, and WECC2012010741 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 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 (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-2284	WECC2012010739	CIP-005-1	R1; R1.1; R1.5; R1.6	Medium	$155,000
			WECC2012010740	CIP-005-3	R4	Medium	
			WECC2012011029	CIP-007-1	R1	Medium	
			WECC2012010439	CIP-007-3a	R2	Medium	
			WECC2012011031	CIP-007-1	R3	Lower	
			WECC2012011329	CIP-007-2a	R4	Medium	
			WECC2012011032	CIP-007-3a	R5; R5.2.3; R5.3.3	Medium	
			WECC2012011034	CIP-007-1	R6	Lower	
			WECC2012010741	CIP-007-3a	R8	Medium	

WECC performed a Compliance Audit of URE (Compliance Audit). During the course of the Compliance Audit, WECC's Audit Team reviewed a series of Self-Reports pertaining to violations of the CIP Reliability Standards that were submitted by URE in the months leading up to the Compliance Audit.

CIP-005-1 R1 (WECC2012010739)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 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."

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity[4] shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
>
> ***
>
> R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
>
> R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical

[4] Within the text of the CIP Standards included in this Notice of Penalty, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-1 R1 has a "Medium" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).[5]

URE submitted a Self-Report stating that it failed to ensure that Cyber Assets used in the electronic access control and monitoring of the Electronic Security Perimeters (ESPs) were afforded the protective measures specified in CIP-005-1 R1.5. WECC determined that URE did not document ports required for normal and emergency operations for 12 Cyber Assets consisting of routers and firewalls. As a result, URE could not ensure that only the ports and services required for normal and emergency operations were enabled on these Cyber Assets as required by CIP-005 R2.

In addition, during the Compliance Audit, WECC determined that URE failed to identify 24 access points to the ESP as required by CIP-005-1 R1.1. Further, WECC determined that URE failed to identify 29 Cyber Assets used in the access control and monitoring of access points, a violation of CIP-005-1 R1.6. The 29 Cyber Assets consisted of servers and appliance devices.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to identify 24 access points to the ESP (R1.1), for failing to ensure 12 Cyber Assets used in the access control and monitoring of the ESPs were afforded the protections of CIP-005 R2.2 (R1.5), and for failing to identify 29 Cyber Assets used in the access control and monitoring of access points (R1.6). All of URE's ESPs were affected.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until mitigated.

WECC determined that this violation poses a moderate risk to the reliability of the bulk power system (BPS), but does not pose a serious or substantial risk. Specifically, URE's failure to identify and afford protections to 65 Cyber Assets located within URE's ESPs rendered those devices vulnerable to exploitation. However, each of the ESPs is equipped with intrusion detection systems (IDS) and access point protections, including externally-connected communication end points. All traffic to and from the ESPs must first pass through firewalls, which are configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices reside within physically secure areas where

[5] WECC assessed the VSL for this violation at the sub-requirement level.

physical access is restricted to individuals with approved Personnel Risk Assessments (PRAs) and access is restricted through the use of key cards.

CIP-005-3 R4 (WECC2012010740)

The purpose statement of Reliability Standard CIP-005-3 provides in pertinent part: "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."

CIP-005-3 R4 provides:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings;
>
> R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-3 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during URE's an annual internal documentation sufficiency review, URE discovered it did not have certain evidence associated with its cyber vulnerability

assessment (CVA) for the previous year. Specifically, URE could not provide documentation demonstrating that it conducted a CVA of 12 electronic access points during that year.

URE reported that insufficient coordination between URE's business teams resulted in URE's failure to perform a CVA on the 12 access points. The electronic access points consisted of routers and firewalls with electronic access to URE's ESPs. URE conducted a full CVA the following year for these access points.

WECC determined that URE had a violation of CIP-005-3 R4 for failing to perform a CVA of all electronic access points to the ESPs at least annually. WECC confirmed that URE's failure to perform a CVA was for the same devices at issue in the CIP-005-1 R1 violation described above (WECC2012010739).

WECC determined the duration of the violation to be for the calendar year that URE missed its CVA.

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 on the 12 access points in question, it did perform a CVA on its other access points. In addition, the affected ESPs were equipped with IDS and access point protections including externally-connected communication end points. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices resided within physically-secure areas where physical access was restricted to individuals with approved PRAs, and access was restricted through use of key cards.

CIP-007-1 R1 (WECC2012011029)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-1 R1 provides:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and

version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.

R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had failed to maintain complete and accurate cyber security control test results for significant changes on Cyber Assets. Specifically, URE reported that after it installed log data collection software, it performed testing on a "non-statistical, judgmental sample of devices." However, it did not perform testing on all covered devices where the software was installed.

During the Compliance Audit, WECC reviewed URE's cyber security test procedures and determined that URE performs cyber security control tests prior to the implementation of new Cyber Assets and when significant changes to existing Cyber Assets occur. However, WECC determined that for 40 Cyber Assets located within two ESPs, URE did not perform complete cyber security control testing after installing the software on those devices. The devices consisted of 27 CCAs and 13 non-critical Cyber Assets.

WECC determined that URE had a violation of CIP-007-1 R1 for failing to ensure all Cyber Assets have complete cyber security control testing and results for all significant changes to Cyber Assets within the ESPs.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that 40 Cyber Assets within two

ESPs were secure following the significant change rendered those devices vulnerable to potential exploitation, potentially allowing unauthorized access to the ESPs. However, URE's networks were isolated from its corporate environment and its internet, and all traffic to and from the ESPs must have first passed through firewalls (which were configured to restrict, monitor, and alert upon suspected malicious activity or traffic). Also, the affected devices resided within physically-secure areas where physical access was restricted to approved, trained, and vetted individuals and access was restricted and monitored through the use of key cards.

CIP-007-3a R2 (WECC2012010439)

The purpose statement of Reliability Standard CIP-007-3a provides in pertinent part: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-3a R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish, document and implement a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
>
> R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).
>
> R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

CIP-007-3a R2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during an annual internal documentation sufficiency review, it discovered that the CVA evidence associated with certain ESPs was deficient. Specifically, URE did

not document ports required for normal and emergency operations for 18 devices. As such, for 9 Critical Cyber Assets (CCAs) and 9 non-critical Cyber Assets, URE could not ensure that only those ports required for normal and emergency operations were enabled.

Subsequently, URE submitted a second Self-Report reporting an increase in the scope of the noncompliance. Specifically, URE found that its CVA did not distinguish ports and services required for normal and emergency operations from all other ports and services. The URE baseline documents for over 500 devices (including approximately 400 CCAs and over 100 non-critical Cyber Assets) did not indicate whether ports and services were required for normal or emergency operations. Because of this failure, URE could not ensure only those ports and services required for normal and emergency operations were enabled.

WECC determined that URE had a violation of CIP-007-3a R2 for failing to enable only those ports and services required for normal and emergency operations. WECC further determined that URE failed to establish a process to ensure that only those ports and services required for normal and emergency operations are enabled. WECC determined that the violation affected over 500 devices used to support all of URE's ESPs.

WECC determined the duration of the violation to be from when URE failed to maintain proper documentation of ports and services through when URE completed its Mitigation Plan.

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that only those ports and services required for normal and emergency operations rendered over 500 devices (and their associated ESPs) vulnerable to potential exploitation, because URE could not ensure that only required ports and services were enabled. However, URE used signature-based filtered IDS to provide protection against attacks, exploits, vulnerabilities, and policy violations. URE's IDS was managed, and the network systems were monitored and activity logged at all times. URE represented that its devices were physically secure, and that it used physical security monitors, identification (ID) badge systems, cameras, guards, and other prevention measures to deter or prevent unauthorized access to its network systems. Further, all individuals with access to URE's ESPs and Physical Security Perimeters (PSPs) had PRAs and proper training.

CIP-007-1 R3 (WECC2012011031)

CIP-007-1 R3 provides:

R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall 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 Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during its pre-audit data request response process, it discovered that it did not have a log or other tracking mechanism for all security patches or all Cyber Assets released during the audit period. Consequently, URE could not establish that it had documented its evaluation of all applicable security patches within 30 calendar days of their availability.

During the Compliance Audit, WECC reviewed URE's Self-Report. WECC determined that while URE used a third-party contractor to perform some security patch management services, a number of Cyber Assets were not covered by this patching program. As a result, URE could not establish that it had documented its evaluation of all applicable security patches within 30 days of availability for nearly 500 Cyber Assets within two ESPs. The devices consisted of approximately 20 CCAs and over 450 non-critical Cyber Assets.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that all Cyber Assets within the ESPs had an established, documented, and implemented security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches put these devices at risk of being compromised by known vulnerabilities. WECC considered that a large number of devices were affected and an unknown number of patches were missed (i.e., each device may have missed multiple patches). However, the affected devices resided within physically-secure areas where physical access was restricted to approved and trained individuals, and where physical access was restricted and monitored through the use of key cards. URE's networks were isolated from its corporate environment and from the internet. Traffic to and from the ESPs must have first passed through firewalls. URE installed anti-virus prevention tools on the affected devices, and the devices were monitored by IDS. In addition, URE filed a Technical Feasibility Exception (TFE) for nearly 80% of these devices, indicating that the manufacturer does not provide patches.

CIP-007-2a R4 (WECC2012011329)

The purpose statement of Reliability Standard CIP-007-2a provides: "Standard CIP-007-2 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-2a R4 provides:

> R4. Malicious Software Prevention —The Responsible Entity shall use anti-virus software and other malicious software ("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 Electronic Security Perimeter(s).
>
> R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-2a R4 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC discovered that URE failed to use anti-virus software and other malicious software prevention tools, where technically feasible, on three Cyber Assets located within two ESPs. Specifically, WECC discovered that one network scanner and two application whitelisting devices did not have anti-virus or malware tools installed when commissioned. The network scanner logged vulnerabilities on the control systems to patch management, and the whitelisting devices prevented the execution of unauthorized code. URE later submitted a TFE, indicating that it was not technically feasible to install anti-virus protection on the two whitelisting devices.

WECC determined that URE had a violation of CIP-007-2a R4 for failing to use anti-virus software and other prevention tools on the network scanner Cyber Asset where prevention tools were technically feasible to install. The network scanner Cyber Asset resided within an ESP.

WECC determined the duration of the violation to be from the day the devices were commissioned 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 affected asset resided within a physically-secure area where physical access was restricted to approved and trained individuals. URE's networks were isolated from its corporate environment and from the internet. All traffic to and from the ESP must have first passed through firewalls. Further, URE installed anti-virus and other malicious software prevention tools on all other capable devices on the affected network, thus ensuring that any virus or malicious software would not go beyond the affected device (had the device been compromised).

CIP-007-3a R5 (WECC2012011032)

CIP-007-3a R5 provides in pertinent part:

R5. Account Management — The Responsible Entity shall 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.

***

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

CIP-007-3a R5 has a "Medium" VRF and a "Severe" VSL.[6]

URE submitted a Self-Report addressing noncompliance with CIP-007-1 R5. Specifically, URE stated that it failed to have a policy for managing the use of shared accounts that could generate an audit trail (R5.2.3).

[6] WECC assessed the VRF at the sub-requirement level.

During the Compliance Audit, WECC determined that for over 500 devices, URE failed to have a policy for managing the use of shared accounts that could generate an audit trail. URE stated that it had controls in place for managing who had access to shared accounts, but no process in place to determine who was using the shared account at any given time. Consequently, URE could not provide evidence of an audit trail of the account use (automated or manual) as required by R5.2.3. The devices included network devices, human machine interfaces, industrial controllers, and printers located in two ESPs.

URE submitted TFEs for this Standard, which WECC approved. As a result, the number of devices associated with this violation was reduced from over 500 to approximately 120 devices. Subsequently, URE submitted amendments to the approved TFEs addressing the feasibility of some of the devices addressed herein. At this time, WECC is reviewing the technical feasibility of URE's devices associated with the amended TFEs.

WECC also determined that URE failed to ensure passwords were changed on an annual basis (R5.3.3). During a CVA, URE identified 13 accounts (10 service accounts and 3 individual user accounts) whose passwords had not been changed in over a year.

WECC determined that URE had a violation of CIP-007-3a R5 for failing to create an audit trail of shared account use (R5.2.3), and for failing to ensure passwords are changed on at least an annual basis (R5.3.3).

WECC determined the duration of the violation to be from the date on which URE mitigated a prior violation of CIP-007-1 R5 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. URE had controls in place for managing who has access to shared accounts, but it failed to establish the technical and procedural controls to manage shared accounts. As a result, URE could not know who was using the shared account at any given time. In addition, URE failed to ensure that passwords were changed on at least an annual basis. However, URE's networks were isolated from its corporate environment and from the internet. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the devices in scope resided within physically-secure areas where physical access was restricted to individuals with approved PRAs and training and where physical access was restricted and monitored through use of key cards. In addition, the devices were actively monitored by IDS.

CIP-007-1 R6 (WECC2012011034)
CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
>
> R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
>
> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that some of its devices were not sending system event logs to URE's centralized logging server, the Security Information and Event Management (SIEM) system. During the Compliance Audit, WECC determined that over 500 devices were affected, consisting of nearly 400 CCAs and over 100 Cyber Assets. The devices included network devices, human machine interfaces, industrial controllers, and printers. The devices were located within two ESPs.

URE stated it had failed to submit TFEs for a large number of devices where it was technically infeasible for the device to implement automated tools to monitor system events that are related to cyber security. Specifically, URE reported that it was technically infeasible to log or monitor system events on over 400 devices. URE reported that over 60 devices were technically capable of logging and monitoring, but were not properly configured to do so.

WECC determined that URE had a violation of CIP-007-1 R6 for failing to ensure that over 500 Cyber Assets within two ESPs were monitoring system events related to cyber security.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement logging and monitoring controls on all of its Cyber Assets could have allowed unauthorized access to those devices to go unnoticed and unchecked, potentially allowing for malicious access. However, the two affected ESPs were equipped with IDS and access point protections including externally connected communication end points. All traffic to and from the ESPs must have first passed through firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the affected devices resided within physically-secure areas where access was restricted to individuals with approved PRAs and training; physical access to these areas was restricted and monitored through use of key cards. Lastly, although URE failed to implement controls on the affected Cyber Assets, URE implemented automated tools and organizational process controls to monitor system events on other Cyber Assets.

CIP-007-3a R8 (WECC2012010741)

CIP-007-3a R8 provides:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. A document identifying the vulnerability assessment process;

R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

R8.3. A review of controls for default accounts; and,

R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-3a R8 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that, during an annual internal documentation sufficiency review, URE discovered that certain evidence associated with its vulnerability assessments was insufficient. Specifically, URE could not identify a formal document that clearly demonstrated that a CVA was performed in the prior calendar year. Consequently, URE did not have documentation of an action plan to remediate or mitigate any vulnerability identified in an assessment.

URE stated it had failed to perform a CVA on 18 devices. Of the 18 devices in scope, 9 devices were CCAs and 9 were non-critical Cyber Assets. The devices resided in URE's ESPs. The devices consisted of routers and switches used to support the networking functions of the ESPs. According to URE, insufficient coordination between its business teams resulted in URE's failure to perform a CVA on certain assets. URE conducted a full CVA in the following year that addressed the CIP-007 R8 requirements.

WECC determined that URE had a violation of CIP-007-3a R8 for failing to perform a CVA of all Cyber Assets within an ESP at least annually. URE's failure to perform its CVA was for the same devices in scope of the CIP-007-3a R2 violation (WECC2012010439) described above.

WECC determined the duration of the violation to be for the calendar year for which the CVA was not performed on the 18 devices.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed a CVA on the remaining Cyber Assets. In addition, the ESPs affected by the violation were equipped with IDS and access point protections, including externally connected communication end points. All traffic to and from the ESPs must have first passed through

firewalls, which were configured to restrict, monitor, and alert upon suspected malicious activity. Further, the 18 affected devices resided within physically-secure areas where physical access was restricted to individuals with approved PRAs and training; physical access was restricted and monitored through use of key cards.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred fifty-five thousand dollars ($155,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. WECC determined that URE's violation history warranted an aggravation of the monetary penalty;
2. URE self-reported the violations of CIP-005-1 R1 (WECC2012010739), CIP-005-3 R4 (WECC2012010740), and CIP-007-3a R8 (WECC2012010741);[7]
3. upon undertaking the actions outlined in its Mitigation Plans, URE took voluntary corrective action to remediate the violations;
4. URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation, which WECC considered a mitigating factor;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. there was no evidence that the violations were intentional;
8. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of one hundred fifty-five thousand dollars ($155,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[7] WECC did not award self-reporting credit for the remaining self-reported violations as the Self-Reports were submitted in the months leading up to the Compliance Audit.

Status of Mitigation Plans[8]

CIP-005-1 R1 (WECC2012010739)

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. complete the implementation of new SIEM systems;
2. complete the implementation of new authentication, authorization, and accounting systems;
3. complete compliance activities for a jump server, existing secure sockets layer virtual private network systems, remote server adapter servers, and intelligent process solutions assets;
4. complete implementation of new log collection devices; and
5. complete compliance activities for active directory and energy management system upgrade.

CIP 005-3 R4 (WECC2012010740)

URE's Mitigation Plan to address its violation of CIP-005-3 R4 was accepted by WECC approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review and update its vulnerability assessment procedure;
2. establish a detailed workbook containing network statistics configuration dates for each affected CIP Cyber Asset;
3. create action plans to identify and document the results of all issues from the following year's CVA and track remediation or mitigation of vulnerabilities;
4. create a summary report for the CVA for the affected CIP Cyber Assets; and
5. conduct a review of overall controls, ports and services, and assessment results with key business and information security personnel.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

[8] *See* 18 C.F.R § 39.7(d)(6).

CIP-007-1 R1 (WECC2012011029)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. clarify its testing procedures to require better documentation;
2. initiate a periodic review of proposed changes and verification of completed significant changes to testing documents; and
3. train employees on how and what to do when performing significant change testing.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R2 (WECC2012010439)

URE's Mitigation Plan to address its violation of CIP-007-3a R2 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review all CVA documentation containing analyses of compiled ports and services and identify those ports and services where the accompanying justifications were not documented;
2. disable listening ports and enabled services that are not required for normal and emergency operations for all Cyber Assets subject to the compliance program at the time the CVA was conducted for all Cyber Assets;
3. for all ports and services that must remain listening and enabled, ensure that justifications are provided for each;
4. review and update its relevant CVA procedure to ensure all requirements are met;
5. establish a detailed workbook containing network statistics configuration data for each affected Cyber Asset;
6. create action plans to identify and document the results of all issues from the vulnerability assessment and track remediation or mitigation of vulnerabilities; and

7. conduct a review of overall controls, ports, services, and assessment results with key business and information security personnel.

URE submitted a Certification of Mitigation Plan Completion. WECC is verifying that URE's Mitigation Plan was completed.

CIP-007-1 R3 (WECC2012011031)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. enhance its patch management program (which includes the review, identification, tracking, and remediation for security patches);
2. have the relevant staff meet to review, approve, and document the review of security patches on its patch review tracking log. The patches are identified as part of the asset and configuration baseline management for every system and the related software.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-2a R4 (WECC2012011329)

URE's Mitigation Plan to address its violation of CIP-007-2a R4 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install anti-virus software on the network scanner Cyber Asset;
2. work with its vendor to test the functionality of the anti-virus software; and
3. work with its vendor to validate the operation of the asset and the anti-virus software after installation of the software.

After WECC's review of URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R5 (WECC2012011032)

URE's Mitigation Plan to address its violation of CIP-007-3a R5 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change or disable all systems accounts passwords and, where applicable, file TFEs for accounts whose passwords could not be changed;
2. create an operators account to eliminate general use by operators of the administrative shared account; and
3. update existing policies and procedures to address specifically the use of existing physical door systems (i.e., badge card readers) and security cameras, as a means to provide an audit trail of the use of the shared accounts.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R6 (WECC2012011034)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify, test, configure, and validate a logging client, including performing testing of the logging client and performing logging against the requirements;
2. implement a process whereby URE generates a monthly log report for certain assets configured with the logging client which is reviewed to confirm that those assets are in fact logging; and
3. identify systems which required TFEs for technical and operational infeasibility and file the appropriate TFEs with WECC.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-3a R8 (WECC2012010741)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review and update its relevant CVA procedure;
2. establish a detailed workbook containing network statistics configuration data for each affected CIP Cyber Asset;
3. create an action plan to identify and document the results of all issues from vulnerability assessments and track remediation and mitigation of vulnerabilities;
4. create a summary report of its CVA for affected Cyber Assets; and
5. conduct a review of overall controls, ports and services, and assessment results.

After reviewing URE's Certification of Mitigation Plan Completion and submitted evidence, WECC verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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,[10] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2014. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred fifty-five thousand dollar ($155,000) financial penalty against URE 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's violation history, which WECC considered an aggravating factor, as described above;

[9] *See* 18 C.F.R. § 39.7(d)(4).

[10] *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).

2. URE self-reported the violations of CIP-005-1 R1 (WECC2012010739), CIP-005-3 R4 (WECC2012010740), and CIP-007-3a R8 (WECC2012010741), which WECC considered a mitigating factor, as described above;
3. upon undertaking the actions outlined in its Mitigation Plans, URE took voluntary corrective action to remediate the violations, which WECC considered a mitigating factor, as described above;
4. WECC reported that URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation, which WECC considered a mitigating factor, as discussed above;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. there was no evidence that the violations were intentional;
8. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. WECC reported that 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 fifty-five thousand dollars ($155,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be Included as Part of this Notice of Penalty

REMOVED FROM THIS PUBLIC VERSION

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

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco*
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Jim Robb*
Chief Executive Officer
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6853
jrobb@wecc.biz

Constance White*
Vice President of Compliance
Western Electricity Coordinating Council
155 North 400 West, Suite 200
Salt Lake City, UT 84103
(801) 883-6885
(801) 883-6894 – facsimile
CWhite@wecc.biz

Ruben Arredondo*
Senior Legal Counsel
Western Electricity Coordinating Council
155 North 400 West, Suite 200

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

Chris Luras*
Director of Compliance Risk Analysis & 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

Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredando@wecc.biz	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/ 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
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

cc: Unidentified Registered Entity
Western Electricity Coordinating Council