PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REDACTED FROM THIS PUBLIC VERSION

October 31, 2012

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. NP13-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because WECC and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of the violations[3] of CIP-002-1[4] R3, CIP-003-1 R6, CIP-004-1 R1, CIP-005-1 R1, R2 and R4, CIP-

[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 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

[4] At the time of URE's violations, Version 1 of the CIP Standards was in effect and was mandatory and enforceable for the entity. CIP Version 1 became effective on July 1, 2008 and remained enforceable through March 31, 2010. CIP Version 2 was approved by the Commission and became enforceable on April 1, 2010 and was enforceable through September 30, 2010. CIP Version 3 was approved by the Commission and became enforceable on October 1, 2010 and remained enforceable through the end duration date of the CIP violations included in this filing. For consistency in this filing, Version 1 of the CIP Standards is used throughout.

006-1 R1,[5] CIP-007-1 R2, R3 and R8, PRC-005-1 R2 and PRC-017-0 R2. According to the Settlement Agreement, URE agrees and stipulates to the facts of the violations and has agreed to the assessed penalty of two hundred thousand dollars ($200,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers WECC201102827, WECC201102715, WECC201002389, WECC201102828, WECC201102830, WECC201002440, WECC201102825, WECC201102823, WECC201002713, WECC201002441, WECC201102897 and WECC201102898 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, by and between WECC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2012), 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-1534	WECC201102827	CIP-002-1	R3	High[6]	$200,000
			WECC201102715	CIP-003-1	R6	Lower	
			WECC201002389	CIP-004-1	R1	Lower	
			WECC201102828	CIP-005-1	R1	Medium[7]	
			WECC201102830	CIP-005-1	R2	Medium[8]	

[5] When Version 2 of CIP-006 was approved, the requirement number for the applicable language was changed. This violation spans multiple versions of CIP-006, and thus includes CIP-006-1 R1.8, CIP-006-2 R2.2, CIP-006-2a R2.2, CIP-006-3a R2.2 and CIP-006-3c R2.2. For consistency in this filing, CIP-006-1 R1.8 is used throughout.
[6] CIP-002-1 R3 has a "High" VRF; CIP-002-1 R3.1. R3.2 and R3.3 each have a "Lower" VRF.
[7] CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; CIP-005-1 R1.6 has a "Lower" VRF.
[8] CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; CIP-005-1 R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			WECC201002440	CIP-005-1	R4	Medium[9]	
			WECC201102825	CIP-006-1	R1	Medium[10]	
			WECC201102823	CIP-007-1	R2	Medium	
			WECC201002713	CIP-007-1	R3	Lower	
			WECC201002441	CIP-007-1	R8	Medium[11]	
			WECC201102897	PRC-005-1	R2	High[12]	
			WECC201102898	PRC-017-0	R2	Lower	

WECC201102827 CIP-002-1 R3

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity[13] shall develop a list of associated

[9] CIP-005-1 R4, R4.2, R4.3, R4.4 and R4.5 each have a "Medium" VRF; CIP-005-1 R4.1 has a "Lower" VRF.
[10] CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; CIP-006-1 R1.7, R1.8 and R1.9 each have a "Lower" VRF. Later versions of CIP-006 R2 and its subrequirements each have a "Medium" VRF.
[11] CIP-007-1 R8 and R8.1 each have a "Lower" VRF; CIP-007-1 R8.2, R8.3 and R8.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation applied to CIP-007-1 R8.2 and 8.3 and a "Medium" VRF is appropriate.
[12] PRC-005-1 R2 has a "Lower" VRF; PRC-005-1 R2.1 and R2.2 each have a "High" VRF. In the context of this case, WECC determined the violation applied to PRC-005-1 R2.1 and R2.2, and a "High" VRF is appropriate.
[13] Within the text of Standards CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, BA, Interchange Authority, TSP, TO, TOP, GO, GOP, LSE, NERC, and Regional Reliability Organizations.

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

[Footnote added.]

CIP-002-1 R3 has a "High" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE self-reported to WECC a violation of CIP-002-1 R3. During an internal review of compliance with the CIP Standards, and in connection with the commencement of its annual review of Critical Cyber Assets (CCAs), URE discovered that it failed to identify 13 CCAs essential to the operation of its Critical Assets (CAs).

URE has two managers who are responsible for identifying CCAs. In addition to the managers, URE also relies on electronic records to identify CCAs and develop lists; however, during its annual review process, URE discovered its lists of CCAs were insufficient. Specifically, 13 devices used for various routing, multiplexor, transmission, switching, and network storage functions were not identified as critical. URE indicated that after implementing a more comprehensive method for asset identification, which included physically verifying records, URE identified the 13 CCAs at issue essential to the operation of the CAs.

WECC determined that URE had a violation of CIP-002-1 R3 for failing to identify 13 CCAs essential to the operation of the CAs.

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

WECC determined that this violation posed a moderate risk and not a serious or substantial risk to the reliability of the bulk power system (BPS). Specifically, failure to identify CCAs could result in leaving the CCA unprotected and vulnerable to a cyber threat and may pose a critical risk to the operation of the BPS. In this instance, URE failed to identify 13 CCAs essential to the operation of the substation, EMS and emergency operations center ESPs. URE's failure to include these CAs on the CCA list could result in the devices being misused or unavailable during CA recovery efforts. As compensating measures, the CCAs in scope were located within identified ESPs and Physical Security Perimeters (PSPs) and were given the protections required in CIP-005-1 and CIP-006-1. In addition, the assets in scope were protected by intrusion detection systems.

WECC201102715 CIP-003-1 R6

The purpose statement of Reliability Standard CIP-003-1 provides: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R6 provides:

> Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R6 has a "Lower" VRF and a "Severe" VSL.

WECC notified URE that WECC was initiating the annual CIP Self-Certification process. URE submitted a Self-Certification citing noncompliance with CIP-003-1 R6. According to the Self-Certification, URE had established and documented a process for change control; however, the process failed to effectively control changes made to its CCA hardware or software. In addition, URE reported it lacked a process that explicitly governs managing configuration changes.

URE's change control process did not require changes to be approved prior to implementation and did not enforce segregation of duties when adding, modifying, replacing, or removing CCA hardware or software. Additionally, URE failed to establish and document a process to control configuration

changes to hardware and software components of CCAs. Consequently, URE's failure to establish and document adequate change control and configuration management procedures resulted in its personnel not following consistent procedures with respect to over 100 CAs and over 100 CCAs. WECC determined that URE's change control process lacked the necessary steps required to fulfill the required activities in CIP-003-1 R6. Specifically, URE's process did not require changes to be approved prior to implementation, did not enforce segregation of duties, and failed to implement procedures for informing personnel of change control and configuration management procedures. Additionally, WECC determined that URE failed to establish and document a configuration management process needed to identify, control, and document all entity or vendor-related changes to hardware and software components of CCAs.

WECC determined that URE had a violation of CIP-003-1 R6 because URE failed to establish and document a program for change control and configuration management that included supporting configuration management activities as required by the Standard.
WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to 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, failure to establish a change control and configuration management process could potentially allow adding or modifying hardware and software changes that could be harmful to CCAs essential to the operation of the BPS, thereby introducing or exposing potential security vulnerabilities to the CCAs. Change control is consistently a high-priority process on several best practice frameworks because ineffective or poor change management can dramatically impact systems. There are over 100 CCAs in scope of URE's existing change control and management procedures that require entity and vendor-initiated changes. The risk to the BPS was mitigated by the following compensating measures: (1) URE's CAs are all located and protected within an ESP and are isolated from the Internet and internally with network segmentation perimeter security including firewalls which deny access by default; (2) URE has intrusion detection and intrusion protection systems to alert for unauthorized access and other security events; (3) remote access from the Internet to the corporate network is only available using two-factor authentication; (4) VPN and/or two-factor authentication is used to access the internal network segments associated with CCAs and CAs; (5) CCAs and CAs are logically secured (cyber access) only to those with a need to know and who are appropriately authorized for access; (6) shared account access to devices on behalf of users is managed; (7) personnel with authorized cyber and/or unescorted physical access have completed personnel risk assessments (PRAs); and (8) to reduce the risk of connection to the Internet (where allowed), anti-virus is in place and updated signatures are applied on a regular schedule where technically feasible. In addition, spam and virus control are in place for email and web browsing.

WECC201002389 CIP-004-1 R1

The purpose statement of Reliability Standard CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R1 provides:

> R1. Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
>
> • Direct communications (e.g., emails, memos, computer based training, etc.);
>
> • Indirect communications (e.g., posters, intranet, brochures, etc.);
>
> • Management support and reinforcement (e.g., presentations, meetings, etc.).

CIP-004-1 R1 has a "Lower" VRF and a "High" VSL.

URE self-reported a violation of CIP-004-1 R1. URE has a security awareness and training policy and a program which requires ongoing security awareness and maintains the required ongoing security reinforcement mechanisms on a quarterly basis. As part of URE's program, it utilizes direct and indirect communication mechanisms to distribute security awareness. Specifically, URE uses emails, newsletters, and the company intranet to distribute its quarterly security awareness updates. For the third and fourth quarters of a year and third quarter of the following year, URE used direct communication via email to distribute reinforcement in sound security practices; however, there were contractors and service vendors who did not receive the email. URE stated further that the failure to distribute the email to all of URE's contractors and service vendors was an oversight since those same individuals were included in previous and subsequent reinforcement mechanisms. WECC determined that URE failed to ensure all authorized personnel receive on-going reinforcement in security awareness. Specifically, URE's failure to distribute quarterly security awareness reinforcement to

contractors and service vendors with physical access to CCAs in several substations is a violation of CIP-004-1 R1.

WECC determined that URE had a violation of CIP-004-1 R1 because URE failed to ensure all authorized personnel received on-going reinforcement in security awareness as required by the Standard.

WECC determined the duration of the violation to be from the date URE failed to deliver quarterly security reinforcement, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because the affected personnel were contractors and service vendors, instead of employees, and had received annual cybersecurity training, had current PRAs, as well as had exposure to prior quarterly security awareness program mechanisms. The contractors affected comprise a small percentage (17%) of the personnel with physical access to CCAs. Further, all of the contractors had been part of the prior security program, a few months earlier. In addition, URE monitors its access control system twenty-four hours a day, seven days a week for unauthorized access attempts or alarms from the PSPs.

WECC201102828 CIP-005-1 R1

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. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity 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).
>
> ***
>
> R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

> 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.

CIP-005-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-005-1 R1. URE discovered that it had failed to identify two non-critical CAs within a defined ESP as required by CIP-005-1 R1.4. These CAs are used for communications located in URE's substation and are part of the substation's ESP. In addition, URE failed to provide protections to several CAs used in the access control and monitoring (ACM) of some ESPs, as required by CIP-005-1 R1.5. Specifically, URE failed to provide the following protections: to make available its change control and configuration management documentation as specified in CIP-003-1 R6; to enable only ports and services required for operations and for monitoring CAs within the ESP as specified in CIP-005 R2.2; and to make available documentation and records of its security patch management program as specified in CIP-007-1 R3.1.

URE's change control process did not require changes to be approved prior to implementation and did not enforce segregation of duties. In addition, the change management procedures were not defined to URE's personnel. Thus, since compliance enforcement date of the Standard, URE's personnel did not follow its established change control and configuration management procedure, and URE lacked a change control and configuration management procedure that met all of the requirements of CIP-003 R6. Further, URE failed to disable ports and services not required for operating and monitoring CAs within the ESP as required of CIP-005 R2, and failed to document the assessment and implementation of security patches as required of CIP-007 R3.

WECC determined that URE had a violation of CIP-005-1 R1 for failing to identify and document all non-critical CAs within a defined ESP as required by R1.4 and for failing to afford protections to CAs used in the ACM of the ESP (R1.5).

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

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because, although the affected CAs were not afforded three of the protections

required by R1.5, they were otherwise treated the same as all other URE CCAs pursuant to CIP-003, CIP-004, CIP-005, CIP-007 and CIP-009. In addition, all other URE CCAs not affected by the violation were afforded the protections of R1.5. Further, each CA was located within a secured PSP and afforded the same protection as all URE CCAs pursuant to CIP-006.

WECC201102830 CIP-005-1 R2

CIP-005-1 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ***
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall
>
> ***

CIP-005-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-005-1 R2. Specifically, URE failed to document enabled ports and services required for operations and for monitoring CAs within the ESP as required by CIP-005-1 R2.2. In addition, URE failed to disable ports and services not required for operations and monitoring of CAs.

URE maintains ports and service configurations for its access points to the ESP on internal documents referred to as "profiles" as part of its process to ensure that only those ports and services required for operations and for monitoring CAs within the ESP are enabled. However, during a vulnerability assessment, URE discovered that on each of its access points, several ports and services were enabled but not documented though the system profile. Specifically, URE failed to document three enabled ports and services that were used to allow printing to printers on the printer network. In addition, URE failed to disable ports and services that should have been removed as part of the annual cyber vulnerability assessment (CVA).

WECC determined that URE had a violation of CIP-005-1 R2.2 for failing to document that it only enabled ports and services required for operations and for monitoring CAs.

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

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because although URE failed to implement and document some access controls, the ESPs in scope were protected by intrusion detection and prevention systems that implement twenty-four hours a day, seven days a week logging and monitoring. In addition, the ports that were compromised were only to printer access and not to the EMS or other key portions of the network.

WECC201002440 CIP-005-1 R4

CIP-005-1 R4 provides in pertinent part:

> 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:
>
> ***
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> ***
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings; and,
>
> ***

CIP-005-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-005-1 R4. URE failed to perform an annual CVA of the electronic access points to the ESP. Additionally, URE failed to verify that only ports and services required for operations at these access points are enabled and failed to assess a review of controls for default accounts, passwords, and network management community strings. URE's CVA policy requires a CVA to be performed at least annually; however, during an internal review, URE discovered that it failed to conduct a CVA for 67% of its access points during a two-year period. For 33% of its access points, URE failed to conduct a review to verify that only ports and services required for operation are enabled and

it failed to administer a review of controls for default accounts, passwords, and network management community strings. These access points are firewalls

WECC determined that URE had a violation of CIP-005-1 R4 for failing to perform an annual CVA of the electronic access points to the ESPs that included a review to verify that only ports and services required for operations at these access points are enabled (R4.2) and failed to review controls for default accounts, passwords, and network management community strings is included in annual vulnerability assessment (R4.4).

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to 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 perform a CVA of all CAs could allow vulnerabilities in such assets to go unchecked and undetected. Subsequently, such vulnerabilities could be exploited by malicious access, thereby allowing undetected unauthorized access at the access points. In this instance, the risk was mitigated because URE had a documented CVA process which included the discovery of all access points to the ESP and documentation of the results of the assessment. These access points in scope allowed only ports and services which have been specifically defined by rules within URE's firewall configuration. As additional compensating measures, URE has intrusion detection systems implemented and access and system logging is in place to detect and prevent unauthorized access.

WECC201102825 CIP-006-1 R1

The purpose statement of Reliability Standard CIP-006-1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> ***

> R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

***

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-006-1 R1. URE failed to ensure two CAs used in the ACM of the PSPs were afforded all the protections required by CIP-006-1 R1.8. Specifically, URE failed to provide to CAs the following protections, as required by the corresponding Standards, used in the ACM of several PSPs:

1) CIP-003 R6: URE established and documented a process for change control; however, the change control process did not require changes to be approved prior to implementation and did not enforce segregation of duties when adding, modifying, replacing, or removing CCA hardware or software. Additionally, URE failed to establish and document a process to control configuration changes to hardware and software components of CCAs. Consequently, URE's failure to establish and document adequate change control and configuration management procedures resulted in its personnel not following consistent procedures in the CAs used in the ACM of the PSPs in scope.

2) CIP-007 R2: URE failed to disable certain ports and services that were not required for normal and emergency operations on its physical access control systems prior to production use of the devices. Specifically, URE failed to disable its its secondary logon service, and another service. In all other cases, services were correctly identified, but the port used by the service as identified on the profile of the device was different on a later scan of the device.

3) CIP-007 R3: URE failed to document an assessment for applicability of security patches within 30 days of the patch being made available for several physical ACM devices. Specifically, software security patches installed on the PAC systems were not assessed within 30 days of the patches being made available.

4) CIP-007 R8: URE's annual CVAs, for a two-year period, failed to review and verify that only ports and services required for operations of specific servers were enabled. In addition, URE failed to implement a review of controls for default accounts for these servers.

WECC determined that URE had a violation of CIP-006-1 R1.8 for failing to ensure that protective measures outlined in CIP-003 R6, CIP-007 R2, CIP-007 R3, and CIP-007 R8 were provided to CAs used in the ACM of the PSPs, as required by the Standard.

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

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because, as a compensating measure, the PSPs in scope had intrusion detection and intrusion protection systems to alert for unauthorized access and other security events. There were no alerts/attacks during the violation duration.

WECC201102823 CIP-007-1 R2

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). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document 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 or an acceptance of risk.

CIP-007-1 R2 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-007-1 R2. Specifically, URE failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled. In addition, URE failed to disable other ports and services. URE documents the ports and service configurations for CAs that reside within an ESP on internal documents referred to as "profiles" as part of its process to ensure that only those ports and services required for normal and emergency operations are enabled; however, during a recent CVA, URE determined that in several instances, ports were enabled on CAs within an ESP, but not documented on the system profile. Specifically, URE failed to ensure that only ports and services required for normal and emergency operations were enabled for 41% of the total CAs located in several substations and ESPs.

WECC determined that URE had a violation of CIP-007-1 R2 because URE failed to establish and document a process to ensure that only ports and services required for normal and emergency operations are enabled as required by the Standard.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to 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 only those ports and services required for normal and emergency operation are enabled poses a risk for unauthorized access to its CAs. This increased risk may allow for unauthorized internal or external access to CAs which could allow for potential cyber attacks against CCAs essential to the operation of the BPS. In this instance, URE failed to ensure that only those ports and services required for normal and emergency operations were enabled for 41% of the CAs. As compensating measures, all devices were protected by anti-virus and anti-malware software, intrusion detection protection systems, and all remote access into the devices required two-factor authentication. There were no events during violation duration, and all access was logged.

WECC201002713 CIP-007-1 R3
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 self-reported a violation of CIP-007-1 R3. URE failed to document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades as required by CIP-007 R3.1. In addition, URE failed to document the implementation of security patches as required by CIP-007 R3.2. URE maintains a cybersecurity policy which requires a security patch management program which implements procedures for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all CAs within the ESPs. As part of this policy, URE assesses security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades. However, during an internal review of compliance with CIP Standards, URE discovered some of the security patches and upgrades installed on the network were not timely assessed. Specifically, URE failed to document the assessment and implementation of security patches for over 100 CAs located in several areas. As a result, WECC determined that URE failed to establish and document a sufficient security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all CAs within the ESPs.

WECC determined that URE had a violation of CIP-007-1 R3 because URE failed to document the implementation and assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

WECC determined the duration of the violation to be from when the assessment of security upgrades did not occur, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because of the following mitigating factors: 1) URE's CAs within an ESP are isolated from the Internet and internally with network segmentation; 2) perimeter security includes firewalls which deny access by default; 3) URE has intrusion detection and protection systems to alert for unauthorized access and other security events; 4) CAs are logically secured (cyber access) only to those with a need to know and appropriately authorized for access; and 5) CAs are physically secured only to those with a need to know and appropriately authorized for access, and all noncompliant visitors are escorted.

WECC201002441 CIP-007-1 R8
CIP-007-1 R8 provides in pertinent part:

> 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:
>
> ***
>
> R8.2. 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;
>
> ***

CIP-007-1 R8 has a “Medium” VRF and a “Severe” VSL.

URE self-reported a violation of CIP-007-1 R8. URE failed to ensure that the annual CVA of CAs in the ESPs included a review to verify that only ports and services required for normal and emergency operation of the CAs within the ESP are enabled (R8.2) and failed to assess a review of controls for default accounts (R8.3). During an internal review of compliance, URE discovered that its annual CVAs, for a two-year period, failed to conduct a review to verify that only ports and services required for normal and emergency operations of CAs within the ESPs are enabled. In addition, URE failed to conduct a review of controls for default accounts for these CAs. In total, over 100 CAs in two ESPs are

in the scope of this violation. Although URE performed an annual CVA for a two-year period, it failed to complete the review requirements of the Standard as specified in R8.2 and R8.3.

WECC determined that URE had a violation of CIP-007-1 R8 because of URE's failure to ensure that the annual CVA of CAs in the ESPs included a review of ports and services and a review of controls for default accounts.

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

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS because as compensating measures, URE had cyber intrusion detection systems and intrusion prevention systems in effect to detect and prevent any cybersecurity event. Also, physical access to the ports and services in scope was given only to personnel with appropriately authorized access and only when needed.

WECC201102897 PRC-005-1 R2

The purpose statement of Reliability Standard PRC-005-1 provides: "To ensure all transmission and generation Protection Systems[14] affecting the reliability of the Bulk Electric System (BES) are maintained and tested."

[Footnote added.]

PRC-005-1 R2 provides:

> R2. Each Transmission Owner and any Distribution Provider that owns a transmission Protection System and each Generator Owner that owns a generation Protection System shall provide documentation of its Protection System maintenance and testing program and the implementation of that program to its Regional Reliability Organization on request (within 30 calendar days). The documentation of the program implementation shall include:
>
> > R2.1. Evidence Protection System devices were maintained and tested within the defined intervals.

[14] *The NERC Glossary of Terms Used in Reliability Standards* defines Protection System as "Protective relays, associated communication systems, voltage and current sensing devices, station batteries and DC control circuitry."

R2.2. Date each Protection System device was last tested/maintained.

PRC-005-1 R2 has a "High" VRF and a "Lower" VSL.

URE self-reported a violation of PRC-005-1 R2. According to the Self-Report, URE maintains telecommunications facilities which have been identified as integral to its transmission Protection Systems. These telecommunication facilities carry a portion of URE's transmission relay traffic. During preparation for a WECC Audit, URE discovered instances where its maintenance and testing records were not consistent with intervals prescribed by its Protection System maintenance and testing Program. Specifically, URE failed to test and maintain battery banks at various sites, and one communication device. Consequently, URE could not produce maintenance and testing records consistent with intervals prescribed under its Protection System maintenance and testing Program. URE reported to WECC that its program requires testing to be performed on batteries every six months. In addition, URE's program requires URE personnel to perform an annual maintenance on the other device. URE submitted maintenance and testing records to WECC; however, URE was not able to provide evidence of maintenance and testing completed within defined intervals for the device and battery banks. During a single year, URE failed to meet the annual interval in one instance for the communication device. Maintenance was performed 268 days behind schedule. In addition, URE failed to meet the six-month battery interval in several instances, ranging from 9 days behind schedule to 45 days behind schedule.

WECC determined that URE had a violation of PRC-005-1 R2 because of URE's failure to perform maintenance and testing on Protection System devices within defined intervals as required by the Standard. 4.7 % of batteries and one communication device were affected by the violation.

WECC determined the duration of the violation to be from when URE failed to complete testing within defined intervals, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS for the following mitigating reasons. URE maintained telecommunications facilities which have been identified as integral to its transmission Protection Systems. These telecommunication facilities carry a portion of URE's transmission relay traffic. This provided a redundant telecommunication backup system. Further, the affected transmission systems were equipped with backup systems to ensure the transmission system will continue to operate without the telecommunications or battery devices at issue. The backup systems are the backup relays that will operate should the primary relays fail or misoperate. These backup systems are able to operate without the telecommunication system. Although URE did not complete testing within defined

intervals, it did complete testing shortly after the defined period, and the missed devices in the systems were verified to operate properly.

WECC201102898 PRC-017-0 R2

The purpose statement of Reliability Standard PRC-017-0 provides: "To ensure that all Special Protection Systems (SPS) are properly designed, meet performance requirements, and are coordinated with other protection systems. To ensure that maintenance and testing programs are developed and misoperations are analyzed and corrected."

PRC-017-0 R2 provides: "The Transmission Owner, Generator Owner, and Distribution Provider that owns an SPS shall provide documentation of the program and its implementation to the appropriate Regional Reliability Organizations and NERC on request (within 30 calendar days)."

PRC-017-0 has a "Lower" VRF and a "Lower" VSL.

URE self-reported a violation of PRC-017-0 R1. URE has a single Special Protection System (SPS). URE's maintenance and testing program that maintains telecommunications systems is part of URE's SPS maintenance and testing program because the telecommunications systems have been identified as associated elements of the SPS, because the telecommunications systems carry input data to the SPS. During preparation for a WECC Audit, URE discovered several instances where maintenance on particular components of these telecommunications facilities was not completed in the defined intervals per URE's maintenance procedure). URE's maintenance procedure requires personnel to perform maintenance on a certain communication device on an annual basis. Additionally, it requires URE personnel to perform maintenance on battery banks every six months. URE failed to meet the annual interval in one instance and the six-month interval several instances, ranging from 9 days behind schedule to 45 days behind schedule.

WECC determined that URE failed to demonstrate that it maintained and tested station batteries at the associated SPS sites within intervals defined in the SPS maintenance procedure. WECC further determined URE has an SPS program; however, URE's failure to maintain and test station batteries at the various communications facilities within the intervals defined in URE's SPS maintenance and testing program resulted in URE not implementing its program.

WECC determined that URE had a violation of PRC-017-0 R1 because URE failed to provide documentation of its SPS maintenance and testing program and its implementation for1.9% of SPS devices.

WECC determined the duration of the violation to be from when URE failed to implement its SPS maintenance and testing program, through when URE completed its Mitigation Plan.

WECC determined that this violation posed a minimal risk and not a serious or substantial risk to the reliability of the BPS. Although URE did not complete testing within defined intervals, it did complete testing shortly after the defined period, and the missed devices in the systems were verified to operate properly. In addition, the affected relay systems had back-up relay systems that will operate without the telecommunications system. The backup systems are the backup relays that will operate should the primary relays fail or misoperate. These backup systems are able to operate without the telecommunication system. Further, maintenance on the affected telecommunications facilities has been completed per URE's testing schedule, and there were no consequences to the BPS during this time of noncompliance.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred thousand dollars ($200,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE received self-reporting credit for all the violations, except for CIP-003-1 R6 WECC201102715;
2. WECC reviewed URE's internal compliance program (ICP) and considered it a mitigating factor in penalty determination;
3. URE was cooperative throughout the compliance enforcement process;
4. URE did not fail to complete any applicable compliance directives;
5. There was no evidence of any attempt by URE to conceal the violations;
6. There was no evidence that URE's violations were intentional;
7. WECC considered some elements of URE's violation history.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred thousand dollars ($200,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[15]

WECC201102827 CIP-002-1 R3
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC on November 8, 2011. The Mitigation Plan was accepted by WECC on November 22, 2011 and approved by NERC on December 20, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update CIP policies and procedures to include annual physical review of devices;
2. Conduct a physical review of devices; and
3. Update the CCA list based on the physical review.

URE certified that the above Mitigation Plan requirements were completed; however, the actual completion date was 161 days past the approved completion date. While URE did update its CCA list per the Mitigation Plan, it failed to date and sign the list until later. As a result, WECC determined the date the list was signed was the completion date.

As evidence of completion of its Mitigation Plan, URE submitted completion evidence documentation.

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

WECC201102715 CIP-003-1 R6
URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to WECC on August 8, 2011. The Mitigation Plan was accepted by WECC on August 25, 2011 and approved by NERC on September 16, 2011. The Mitigation Plan was submitted as non-public information to FERC on September 16, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to complete a full review and process improvement of all documents related to the current change control processes. This review included verification that the following considerations are included in the process:

1. Review documentation of the individuals requesting changes, as well as individuals involved in any aspect of the change process. The process requires that these individuals or roles be different than those approving the change;

[15] *See* 18 C.F.R § 39.7(d)(7).

2. Review documentation that identifies the change that is occurring, the assets being changed, and the impact of the change;
3. Implement a process for reviewing the change plan, change control program and change management documentation of the change.
4. Implement a full review and process improvement of all documents related to configuration management.
5. Train appropriate personnel on the new processes for change control and configuration management; and
6. Review of all configuration documentation to ensure that it is included in the configuration management data list for all CCAs.

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

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

WECC201002389 CIP-004-1 R1

URE's Mitigation Plan to address its violation of CIP-004-1 R1 was submitted to WECC on March 9, 2011. The Mitigation Plan was accepted by WECC on March 18, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan was submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to implement the following actions:

1. Place CIP cyber-awareness posters at all CIP substation PSPs and high-traffic areas where contractors can view them easily. Also, post a laminated copy of URE's visitor management program;
2. Install CIP awareness boards in the substations, where all personnel with physical access can easily view and identify the materials. All CIP information normally presented in electronic format was printed and posted on the boards by URE's security office;
3. Conduct face-to-face training with all contractors reporting to the security offices, as well as any contractors or employees who come to the security offices for replacement badges;
4. Transfer all CIP security awareness to corporate communications; and
5. Add procedures for the maintenance of awareness efforts in all CIP locations.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. Attestation from security services management;
2. Confirmation email from security services management;
3. Completed badge holder checklists, signed by contractors;
4. Meeting invite and notes for meeting;
5. URE's security awareness distribution procedure; and
6. URE's quarterly awareness efforts, presented in the following order:
    a. Copy of newsletter article;
    b. Screen shot of intranet page;
    c. Email to all employees;
    d. Email and attachment to supervisors;
    e. Image of security awareness boards; and
    f. Email confirming boards were updated.

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

WECC201002828 CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to WECC on October 28, 2011. The Mitigation Plan was accepted by WECC on November 28, 2011 and approved by NERC on December 20, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders. On December 22, 2011 WECC issued a notice of extension request acceptance to URE for CIP-005-1 R1 with a revised Mitigation Plan completion date of January 31, 2012.

URE's Mitigation Plan required URE to:

1. For CIP-005-1 R1.4, follow the defined method for asset identification, including physical walk-down of the CA sites and completion of a change control change plan. This resulted in a complete and accurate documented inventory;

2. For CIP-005-1 R1.5, where the Standard requires that ACM assets be afforded the protection of CIP-003 R6, complete the following applicable steps from URE's previously submitted CIP-003-1 R6 Mitigation Plan, discussed above, to correct the violation. URE performed a full review and process improvement of all documents related to the current change control processes. The review included documentation that identifies the change that is occurring, the assets being changed, and the impact of the change;
3. Train appropriate personnel on the new processes for change control and configuration management;
4. Review all configuration documentation to ensure that it includes configuration management data for all ACM assets;
5. For CIP-004-1 R1.5, where the Standard requires that ACM assets be afforded the protection of CIP-005-1 R2.2, identify the ports as not needed were closed as documented on two procedures. Completion of this step resulted in full verification and documentation of the ports and services for all ACM devices; and
6. Complete implementation and training of all personnel on the new system and process.

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

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

WECC201102830 CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to WECC on October 28, 2011. The Mitigation Plan was accepted by WECC on November 28, 2011 and approved by NERC on December 20, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Install new access points as part of an upgrade and complete CVAs utilizing new vulnerability processes completed as part of the CIP-005-1 R4 Mitigation Plan, discussed below; and
2. Complete the installation and cut over to the new firewalls.

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

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

WECC201002440 CIP-005-1 R4

URE's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to WECC on May 23, 2011. The Mitigation Plan was accepted by WECC on July 7, 2011 and approved by NERC on July 25, 2011. The Mitigation Plan was submitted as non-public information to FERC on July 27, 2011 in accordance with FERC orders.

URE's Mitigation Plan required WECC to:

1. Conduct a CVA for access points in scope;
2. Upgrade its EMS system which will identify new access points;
3. Update the CVA process to ensure that all requirements required by CIP-005 R4 are being fulfilled;
4. Train the EMS personnel on the updated procedures; and
5. Conduct the CVA for the new access points.

URE certified that the above Mitigation Plan requirements were completed one day past the approved completion date. As evidence of completion of its Mitigation Plan, URE submitted completion evidence documentation.

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

WECC201102825 CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC on October 28, 2011. The Mitigation Plan was accepted by WECC on December 8, 2011 and approved by NERC on December 21, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders. On December 22, 2011 WECC issued a notice of extension request acceptance to URE for CIP-006-1 R1 with a revised Mitigation Plan completion date of January 31, 2012.

URE's Mitigation Plan required URE to conduct full review and process improvement of all documents related to the current change control processes. Review included verification that the following considerations were included in the process:

1. Review documentation of the individual requesting changes, as well as individuals involved in any aspect of the change process. The process requires that these individuals or roles be different than those approving the change;
2. Review documentation that identifies the change that is occurring, the assets being changed, and the impact of the change;
3. Implement a process for reviewing the change plan, change control program and change management documentation of the change.
4. Implement a full review and process improvement of all documents related to configuration management.
5. Train appropriate personnel on the new processes for change control and configuration management;
6. Complete implementation and training of all personnel on the new system and process;
7. Revise and/or update URE's procedural documents to improve the process for completing and documenting the results of vulnerability assessments; and
8. Train all appropriate personnel on the new processes.

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

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

WECC201102823 CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC on October 28, 2011. The Mitigation Plan was accepted by WECC on December 8, 2011 and approved by NERC on December 21, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Replace all devices as part of URE's EMS upgrade;
2. Ensure that new devices have properly documented ports and services profiles, as defined in the new configuration management processes developed as part of a process improvement effort associated with the CIP-003-1 R6 Mitigation Plan, discussed above. To reduce risk and as part of the Mitigation Plan submitted for CIP-007-1 R8, discussed below, high risk devices were

scanned and open ports and services reviewed to make sure they are properly documented, and any unneeded ports and services are closed; and

3. File Technical Feasibility Exceptions, which were accepted by WECC, for all identified assets affected by the R2.2 violation.

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

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

WECC201002713 CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC on May 23, 2011. The Mitigation Plan was accepted by WECC on July 15, 2011 and approved by NERC on August 24, 2011. The Mitigation Plan was submitted as non-public information to FERC on August 25, 2011 in accordance with FERC orders. On December 22, 2011 WECC issued a notice of extension request acceptance to URE for CIP-007-1 R3 with a revised Mitigation Plan completion date of January 31, 2012.

URE's Mitigation Plan required URE to:

1. Complete the inventory of software whose patches need to be assessed. Include for each device a list of all installed applications or firmware with vendor name and version number;
2. Select an outside consultant to implement a patch assessment process;
3. Revise the CIP patch management process to represent the automated process. Include gap analysis and manual processes for those updates which cannot be managed through the new system.
4. Complete implementation and training of all personnel on the new system and process; and
5. Complete an assessment of all available patches and firmware per the new process and within 30 days of release.

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

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

WECC201002441 CIP-007-1 R8

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to WECC on May 23, 2011. The Mitigation Plan was accepted by WECC on July 7, 2011 and approved by NERC on December 20, 2011. The Mitigation Plan was submitted as non-public information to FERC on December 22, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise and/or update URE's procedural documents to improve the process for completing and documenting the results of CVAs;
2. List documents that will be reviewed, updated and/or developed, as needed, including CVA policies, procedures and test criteria, and a vendor attestation.
3. Train all appropriate personnel on the new processes;
4. Use the new processes to perform a CVA on all substation ESPs and on the new EMS prior to commissioning the new EMS CAs and CCAs within the new EMS ESPs. Completion of such CVAs shall serve as the new bookend dates by which to measure the next required annual CVA required to be performed under URE's cybersecurity policies; and
5. Complete the installation and cut over to the new EMS.

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

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

WECC201102897 PRC-005-1 R2

URE's Mitigation Plan to address its violation of PRC-005-1 R2 was submitted to WECC on August 18, 2011. The Mitigation Plan was accepted by WECC on August 19, 2011 and approved by NERC on September 13, 2011. The Mitigation Plan was submitted as non-public information to FERC on September 14, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete battery maintenance and communication device maintenance;

2. Task an employee to coordinate records for two departments. This employee's primary responsibility is to monitor and record all maintenance for both departments. This will ensure consistency in the records between the departments and prevent oversights. This employee will also assist a supervisor and group leader in coordinating maintenance scheduling;
3. Assign a new compliance specialist. This employee's full time job is to review all NERC maintenance records for three departments; and
4. Task the compliance specialist to review all source documents on completed maintenance and produce a monthly report, rather than a quarterly report produced with a sample of source documents.

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

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

WECC201102898 PRC-017-0 R2

URE's Mitigation Plan to address its violation of PRC-017-0 R2 was submitted to WECC on August 18, 2011. The Mitigation Plan was accepted by WECC on August 19, 2011 and approved by NERC on September 13, 2011. The Mitigation Plan was submitted as non-public information to FERC on September 14, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Task an employee to coordinate records for the two identified departments. This employee's primary responsibility is to monitor and record all maintenance for both departments. This will ensure consistency in the records between the departments and prevent oversights. This employee will also assist a supervisor and group leader in coordinating maintenance scheduling;
2. Assign a new compliance specialist. This employee's full time job is to review all NERC maintenance records for three departments; and
3. Task the compliance specialist to review all source documents on completed maintenance and produce a monthly report, rather than a quarterly report produced with a sample of source documents.

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

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[16]

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,[17] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 10, 2012. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a two hundred thousand dollar ($200,000) 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;
2. URE self-reported 11 of the violations;
3. WECC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had an ICP at the time of the violations which WECC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[16] *See* 18 C.F.R. § 39.7(d)(4).
[17] *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).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred thousand dollars ($200,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be Included as Part of this Notice of Penalty

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

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

b) Record documents for the violation of CIP-002-1 R3, included as Attachment b:

   1. URE's Self-Report;
   2. URE's Mitigation Plan;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-003-1 R6, included as Attachment c:

1. URE's Self-Certification;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-004-1 R1, included as Attachment d:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-005-1 R1, included as Attachment e:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-005-1 R2, included as Attachment f:

1. URE's Self-Report
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-005-1 R4, included as Attachment g:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-006-1 R1, included as Attachment h:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-007-1 R2, included as Attachment i:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-007-1 R3, included as Attachment j:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-007-1 R8, included as Attachment k:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

l) Record documents for the violation of PRC-005-1 R2, included as Attachment l:

1. URE's Self-Report;
2. URE's Mitigation Plan
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

m) Record documents for the violation of PRC-017-0 R2, included as Attachment m:

1. URE's Self-Report;
2. URE's Mitigation Plan;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

A Form of Notice Suitable for Publication[18]

A copy of a notice suitable for publication is included in Attachment n.

[18] *See* 18 C.F.R § 39.7(d)(6).

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 Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6855 (801) 883-6894 – facsimile CWhite@wecc.biz	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonça Attorney North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Christopher Luras* Director of 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

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	*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/ Rebecca J. Michael

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

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonça
Attorney
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments