September 28, 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. NP12-_-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 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-003-1, CIP-004-1, CIP-005-2, CIP-007-1, CIP-008-2 and CIP-009-1.[4] According to the Settlement Agreement, URE agrees and

[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] Based on the durations of the CIP-003, CIP-004, CIP-007 and CIP-009 violations, the violations involved Versions 1, 2 and 3 of the Standards. The Settlement Agreement and this Notice of Penalty refer to Version 1 of CIP-003, CIP-004, CIP-007 and CIP-009 when addressing these violations because the versions involved are substantially similar. Based on the durations of the CIP-005 violations, the violations involved Versions 1, 2, 3 and 3a of the Standard and based on the duration of the CIP-008 violation, the violation involved Versions 2 and 3 of the Standard. The Settlement Agreement and this Notice of

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 WECC201002338, WECC201002339, WECC201002361, WECC201002362, WECC201002363, WECC201002364, WECC201002341, WECC201002342, WECC201002343, WECC201002344, WECC201002345, WECC201002346, WECC201002347, WECC201002348, WECC201002365, WECC201002349 and WECC201002350 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 on February 10, 2012, which is included as Attachment a, as well as the Addendum to the Settlement Agreement executed on June 12, 2012, which is included as Attachment b, 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 (2011), 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-1262	WECC201002338	CIP-003-1	R6	Lower	$200,000
			WECC201002339	CIP-004-1	R2	Medium[5]	
			WECC201002361	CIP-005-2	R1	Medium[6]	

Penalty refer to Version 2 of CIP-005 and CIP-008 when addressing these violations because the versions involved are substantially similar.

[5] CIP-004-1 R2, R2.2.1, R2.2.2, R2.2.3 and R2.3 each have a "Lower" VRF; CIP-004-1 R2.1, R2.2 and R2.2.4 each have a "Medium" VRF. In the context of this case, WECC determined the violation related to R2.1, R2.2 and all its subrequirements and R2.3, and therefore a "Medium" VRF is appropriate. When NERC filed VRFs it originally assigned CIP-004-1 R2.1 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "Medium" VRF, and on January 27, 2009, the Commission approved the modified "Medium" VRF. Therefore, the "Lower" VRF for CIP-004-1 R2.1 was in effect from June 18, 2007 until January 27, 2009, when the "Medium" VRF became effective.

[6] CIP-005-2 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; CIP-005-2 R1.6 has a "Lower" VRF.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			WECC201002362	CIP-005-2	R2	Medium[7]	
			WECC201002363	CIP-005-2	R3	Medium	
			WECC201002364	CIP-005-2	R4	Medium[8]	
			WECC201002341	CIP-007-1	R1	Medium[9]	
			WECC201002342	CIP-007-1	R3	Lower	
			WECC201002343	CIP-007-1	R4	Medium	
			WECC201002344	CIP-007-1	R5	Medium[10]	
			WECC201002345	CIP-007-1	R6	Medium[11]	
			WECC201002346	CIP-007-1	R7	Lower	
			WECC201002347	CIP-007-1	R8	Medium[12]	
			WECC201002348	CIP-007-1	R9	Lower	
			WECC201002365	CIP-008-2	R1	Lower	
			WECC201002349	CIP-009-1	R1	Medium	
			WECC201002350	CIP-009-1	R3	Lower	

CIP-003-1 R6 (WECC201002338)

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."

[7] CIP-005-2 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; CIP-005-2 R2.5 and its subrequirements and R2.6 each have a "Lower" VRF.
[8] CIP-005-2 R4, R4.2, R4.3, R4.4 and R4.5 each have a "Medium" VRF; CIP-005-2 R4.1 has a "Lower" VRF.
[9] CIP-007-1 R1 and R1.1 each have a "Medium" VRF; CIP-007-1 R1.2 and R1.3 each have a "Lower" VRF.
[10] CIP-007-1 R5, R5.1.1, R5.1.2, R5.2, R5.2.2, R5.3, R5.3.1 and R5.3.2 each have a "Lower" VRF; CIP-007-1 R5.1, R5.1.3, R5.2.1, R5.2.3 and R5.3.3 each have a "Medium" VRF. WECC determined the violation related to R5.1, R5.2, R5.3 and all the associated subrequirements, and therefore a "Medium" VRF is appropriate.
[11] CIP-007-1 R6, R6.4 and R6.5 each have a "Lower" VRF; CIP-007-1 R6.1, R6.2 and R6.3 each have a "Medium" VRF. WECC determined the violation related to R6.1, R6.2, R6.3, R6.4 and R6.5, and therefore a "Medium" VRF is appropriate.
[12] 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. WECC determined the violation related to R8, R8.1, R8.2, R8.3 and R8.4, and therefore a "Medium" VRF is appropriate.

CIP-003-1 R6 provides:

> R6. 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" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).[13]

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE reported that its change control and configuration management procedures did not track the appropriate configuration items. Specifically, URE's testing of security controls was limited and did not include the testing of all relevant controls. However, its policy did require management of entity-initiated and vendor-initiated changes. A few months later, WECC conducted an on-site compliance audit of URE's facilities (Audit), during which a URE compliance employee stated that the root cause of the violation was a misinterpretation of the compliance requirements for CIP-003-1 R6.

WECC determined that URE was in violation of CIP-003-1 R6 because it did not establish and document a process of change control and configuration management to identify, control, and document all entity-related or vendor-related changes to hardware and software components of Critical Cyber Assets (CCAs).

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

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the failure to establish a change control and configuration management process could potentially allow adding or changing hardware

[13] On the start date of the violation, no VSLs were in effect for CIP-003-1. On June 30, 2009, NERC submitted VSLs for the CIP-002-1 through CIP-009-1 Reliability Standards. On March 18, 2010, the Commission approved the VSLs as filed, but directed NERC to submit modifications.

and software that could be harmful to CCAs essential to the operation of the bulk electric system, thereby introducing or exposing potential security vulnerabilities to the CCAs. However, the risk was mitigated because URE had change control and management procedures that required management and testing of entity-initiated and vendor-initiated changes, although those procedures were incomplete.

CIP-004-1 R2 (WECC201002339)

The purpose statement of Reliability Standard CIP-004-1 provides: "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 R2 provides:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.
>
> R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:
>
> R2.2.1. The proper use of Critical Cyber Assets;
>
> R2.2.2. Physical and electronic access controls to Critical Cyber Assets;
>
> R2.2.3. The proper handling of Critical Cyber Asset information; and,
>
> R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets
>
> and access thereto following a Cyber Security Incident.
>
> R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

CIP-004-1 R2 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation.

According to URE, it failed to establish, maintain and document an annual cybersecurity training program for personnel having authorized cyber or authorized unescorted physical access to CCAs, and to review the program annually and update as necessary. Although URE conducted annual cybersecurity training for personnel having authorized cyber or authorized unescorted physical access to CCAs, because of the lack of structure and documentation of the program, URE could not demonstrate that training occurred prior to providing access, or that training occurred annually, as required by CIP-004-1 R2. Because the majority of individuals received grandfathered access, URE could not provide evidence that the individuals had training within ninety days of receiving access to CCAs, as required by R2.1. Thirty individuals were not trained within ninety days of receiving unescorted physical or electronic access to CCAs, and received training approximately 110 days after receiving access to CCAs. One additional individual with access to CCAs was not trained. Therefore, the WECC subject matter expert determined that URE's training program did not address the subrequirements of R2.2: *i.e.*, the proper use of CCAs (R2.2.1); the physical and electronic access controls to CCAs (R2.2.2); the proper handling of CCA information (R2.2.3); and action plans and procedures to recover or re-establish CCAs and access thereto following a cybersecurity incident (R2.2.4). In addition, URE could not provide evidence of annual training, as required by R2.3. WECC Enforcement confirmed these findings.

WECC determined the duration of the violation to be from the first day following Certification of Mitigation Plan Completion for a prior CIP violation of URE 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 because the majority of the employees that received access were grandfathered and already had experience with the CCAs. Further, all of the URE employees missing training, with the exception of one employee, performed the required training within 110 days, 20 days beyond the requirement.

CIP-005-2 R1 (WECC201002361), CIP-005-2 R2 (WECC201002362), CIP-005-2 R3 (WECC201002363), CIP-005-2 R4 (WECC201002364)

The purpose statement of Reliability Standard CIP-005-2 provides: "Standard CIP-005-2 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-005-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-005-2 R1 provides:

> 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).
>
> R1.1. 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).
>
> R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
>
> R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security 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-005-2.
>
> R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security
> Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirement R3; Standard CIP-007-2 Requirements R1 and R3 through R9; Standard CIP-008-2; and Standard CIP-009-2.
>
> R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical 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-005-2 R1 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation.

According to URE, its procedure for documenting Electronic Security Perimeters (ESPs) was inadequate and therefore led to many non-critical systems being designated as CCAs. Further, URE's identification and documentation process for access points resulted in a lack of clear documentation of all access points and their associated technical and procedural controls. Lastly, URE failed to develop dial-up security procedures, although it did not have any dial-up access points, and failed to address protective measures for access control and monitoring (ACM) systems.

WECC determined that URE was in violation of CIP-005-2 R1 because URE failed to have adequate documentation to ensure that every CCA resides within an ESP. Additionally, URE failed to identify and document the ESP and all access points to the perimeters.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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 identify and document CIP-compliant ESPs along with the defined access points to an ESP can expose URE's CCAs to significant cybersecurity risks and impact the reliable operation of the BPS. Access points are recognized as an electronic "first line of defense" and serve as security "gatekeepers" for CCAs. However, WECC determined that this violation did not pose a serious or substantial risk because all CCAs were within an ESP. URE's failure to properly identify CCAs resulted in non-critical systems being designated as CCAs and incorrectly protected within an ESP; however, both non-critical systems and CCAs were within an ESP and therefore received some level of protection.

CIP-005-2 R2 provides:

> 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).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

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 document, individually or by specified grouping, the configuration of those ports and services.
R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
R2.5. The required documentation shall, at least, identify and describe:
R2.5.1. The processes for access request and authorization.
R2.5.2. The authentication methods.
R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-2 Requirement R4.
R2.5.4. The controls used to secure dial-up accessible connections.
R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-2 R2 has a "Medium" VRF and a "Severe" VSL.[14]

WECC notified URE that WECC was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE's controls at access points were not fully documented, the list of approved ports and services for each device was not consistently maintained, and no procedure existed for securing dial-up access.

WECC determined that URE was in violation of CIP-005-2 R2 because URE failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all access points to the ESPs.

[14] Each of the requirements and subrequirements of CIP-005-2 R2, with the exception of R2.6, has an assigned VSL of "Severe." These are considered binary requirements, where every violation is assigned a "Severe" VSL.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE 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 because URE had controls in place at the time of the violation, including firewalls and rule sets, although those controls were not well-documented. In addition, although URE did not document a procedure for dial-up access, no dial-up access existed to the ESP.

CIP-005-2 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
>
> R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-2 R3 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE's log monitoring process was insufficient in that it did not define the alert mechanism, or when logs are monitored. These alerts notified the designated response personnel. URE deployed servers to log and monitor its systems, but due to lack of clear procedural guidance, these particular servers were not reviewed and documented consistently.

WECC determined that URE was in violation of CIP-005-2 R3 because URE failed to implement and document an electronic or manual process for monitoring and logging access at access points to the ESPs twenty-four hours a day, seven days a week.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE 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 because URE utilized particular servers to log and monitor its systems, although the servers were not reviewed and documented consistently.

CIP-005-2 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-005-2 R4 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. The information provided on the form showed that URE did not have a detailed process for documenting cyber vulnerability assessments. The form addressed neither the services required for normal and emergency operations, nor the requirement of discovery of access points, nor review community strings.

WECC determined that URE was in violation of CIP-005-2 R4 because URE failed to perform a cyber vulnerability assessment of the electronic access points to the ESP at least annually.

WECC determined the duration of the violation to be the date the Standard became mandatory and enforceable for 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. URE's failure to perform a cyber vulnerability assessment of the electronic access points to the ESPs makes URE unaware of vulnerabilities, and could allow undetected unauthorized access at the access points. However, URE did have a form for documenting vulnerability assessments at the time of the violation, although URE lacked a detailed procedure for performing annual cyber vulnerability assessments.

CIP-007-1 R1 (WECC201002341), CIP-007-1 R3 (WECC201002342), CIP-007-1 R4 (WECC201002343), CIP-007-1 R5 (WECC201002344), CIP-007-1 R6 (WECC201002345), CIP-007-1 R7 (WECC201002346), CIP-007-1 R8 (WECC201002347), CIP-007-1 R9 (WECC201002348)

The purpose statement of Reliability Standard CIP-007-1 provides: "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 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.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to document test procedures to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. URE based its existing procedure on a form that lacks key elements of the requirement. The procedure addresses testing but does not cover all necessary security controls and does not specify how this testing is documented.

WECC determined that URE was in violation of CIP-007-1 R1 because URE failed to document test procedures to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls.

WECC determined the duration of the violation to be from the first day following Certification of Mitigation Plan Completion for a prior CIP violation of 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 testing procedures lacked key elements required by the Standard and could have allowed untested and potentially malicious changes to be released in the production systems. In addition, lack of cybersecurity test procedures could have resulted in a failure to detect and prevent potentially harmful modifications to existing security controls for CCAs. Such modifications could have introduced cybersecurity vulnerabilities into the CCAs essential to the operation of the BPS. If exploited, such vulnerabilities could have negatively impacted the normal operation of the BPS. As a compensating measure, URE's procedure did address testing to minimize adverse effects on the production system, although it did not cover all necessary security controls.

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.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the ESP(s). URE did not have an adequate program to correctly track and assess security patches across all CCA and ACM systems. Because there was no clear procedural guidance, URE was not performing patch assessments within thirty days of release by the vendor.

WECC determined that URE was in violation of CIP-007-1 R3 because URE failed to establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the ESPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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 establish and document a security patch management program could result in vulnerabilities remaining unaddressed for extended periods of time. Security patches are designed to update and protect an asset, and to correct a weakness or vulnerability from exploitation. This increases the risk of a vulnerability being used to launch a successful cyber attack against CCAs essential for operation of the BPS, thereby disrupting the operation of the BPS. However, URE had compensating measures in place at the time of the violation which reduced the risk to the BPS. URE's Cyber Assets received the protections provided by their being located in an ESP and Physical Security Perimeter (PSP). Additionally, all personnel who had access to URE's CCAs had personnel risk assessments (PRAs) and CIP training.

CIP-007-1 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 or an acceptance of risk.
>
> 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-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to 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 ESPs. URE did not document and implement anti-virus and malware software and did not document and implement a process for updating, testing and installing anti-virus and malware signatures.

WECC determined that URE was in violation of CIP-007-1 R4 because URE failed to use anti-virus software and other malware prevention tools, where technically feasible, and failed to document and implement anti-virus and malware software and a process for updating, testing and installing anti-virus and malware signatures.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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, UREs failure to use anti-virus software and other malware prevention tools could allow existing and/or new malicious software, originating from a

security patch, service pack, vendor release, application or database update *etc.*, to be introduced to its Cyber Assets, thereby introducing cybersecurity vulnerabilities into the CCAs essential to the operation of the BPS. If exploited, such vulnerabilities could negatively impact the normal operation of the BPS. However, URE had compensating measures in place at the time of the violation which reduced the risk to the BPS. URE's Cyber Assets received the protections provided by their being located in an ESP and PSP. Additionally, all personnel who had access to URE's CCAs had PRAs and CIP training.

CIP-007-1 R5 provides:

> 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.
>
> R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
>
> R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
>
> R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
>
> R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
>
> 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).

R5.3. At a minimum, the Responsible Entity shall require and use passwords, subject to the following, as technically feasible:

R5.3.1. Each password shall be a minimum of six characters.

R5.3.2. Each password shall consist of a combination of alpha, numeric, and "special" characters.

R5.3.3. Each password shall be changed at least annually, or more frequently based on risk.

CIP-007-1 R5 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to 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. Specifically, URE failed to establish procedures to generate logs of sufficient detail to create historical audit trails for user activity for a number of Cyber Assets in the energy management system (EMS) ESP. Further, URE failed to change passwords for several shared accounts within seven days per its internal password policy. Lastly, URE failed to change passwords annually for several accounts.

WECC determined that URE was in violation of CIP-007-1 R5 because URE failed to 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.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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 establish technical and procedural controls to authenticate and account for user activity for system access could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. Such access may then be used to cause harm to CCAs essential to the operation of the BPS, thereby potentially negatively impacting the BPS. However, URE had compensating measures in places at the time of the violation which reduced the risk to the BPS. URE's Cyber Assets received the

protections provided by their being located in an ESP and PSP. Additionally, all personnel who had access to URE's CCAs had PRAs and CIP training.

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 "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cybersecurity. Specifically, URE's system log server failed to capture logs under heavy volume, failed to retain logs for at least ninety days, and failed to review and document the review of the logs. URE was reviewing security event logs but did not document these reviews. URE's process to document the review of security events was insufficient; therefore log review documentation was inconsistent.

WECC determined that URE was in violation of CIP-007-1 R6 because URE failed to ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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 security controls to monitor cybersecurity system events could allow unauthorized access to the Cyber Assets to go unnoticed and unchecked, potentially allowing malicious access to these assets. In addition, such access may then be used to cause harm to CCAs essential to the operation of the BPS, thereby potentially negatively impacting the BPS. As a compensating measure, URE reported that it reviews logs of system events related to cybersecurity, although the reviews were not documented consistently.

CIP-007-1 R7 provides:

> R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005.
>
> R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
>
> R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
>
> R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

CIP-007-1 R7 has a “Lower” VRF and a “Moderate” VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was “substantially compliant,” it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. Although URE's procedures addressed the disposal of Cyber Assets, the procedures did not document redeployment of Cyber Assets or erasing stored media prior to redeployment.

WECC determined that URE was in violation of CIP-007-1 R7 because URE failed to establish formal methods, processes, and procedures for redeployment of Cyber Assets within the ESPs.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE 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 because although URE did not have clear procedures for its redeployment of Cyber Assets within the ESP, URE did have procedures in place for the disposal of Cyber Assets within the ESP, to ensure that information stored on discarded Cyber Assets could not be used to obtain access to CCAs and potentially disrupt the operation of the BPS.

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

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually. Specifically, URE failed to conduct the vulnerability assessment process annually, which includes documenting the vulnerability assessment process, and reviewing ports, services, and controls for default accounts.

WECC determined that URE was in violation of CIP-007-1 R8 because URE failed to perform a cyber vulnerability assessment of all Cyber Assets within the ESP at least annually.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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 conduct a cyber vulnerability assessment of all Cyber Assets could allow cyber vulnerabilities in such assets to go unchecked and undetected. Subsequently, such vulnerabilities could be exploited by malicious access, thereby providing an attack vector for launching cyber attacks against CCAs essential to the operation of the BPS, thereby disrupting the operation of the BPS. However, URE had compensating measures in place at the time of the violation which reduced the risk to the BPS. URE's Cyber Assets received the protections provided by their being located in an ESP and PSP. Additionally, all personnel who had access to URE's CCAs had PRAs and CIP training.

CIP-007-1 R9 provides: "Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change."

CIP-007-1 R9 has a "Lower" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE failed to review and update the documentation specified in Standard CIP-007 at least annually. URE lacked a documented procedure for document review and maintenance. Because the review and maintenance process was not proceduralized, document owners reviewed and maintained documents per their own schedules, leading to inconsistent results and a failure to maintain and review documents per the Standard. In addition, changes resulting from modifications to the systems or controls were not documented within ninety calendar days of the change.

WECC determined that URE was in violation of CIP-007-1 R9 because URE failed to review and update the documentation specified in Standard CIP-007 at least annually.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for 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, because URE has not defined methods, processes, and procedures for securing its systems determined to be CCAs, as well as the non-CCAs within the ESPs, it cannot review and update the necessary documentation to comply with the Standard. However, URE had compensating measures in place at the time of the violation which reduced the risk to the BPS. URE's Cyber Assets received the protections provided by their being located in an ESP and PSP. Additionally, all personnel who had access to URE's CCAs had PRAs and CIP training.

CIP-008-2 R1 (WECC201002365)

The purpose statement of Reliability Standard CIP-008-2 provides: "Standard CIP-008-2 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-008-2 R1 provides:

> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
>
> R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
>
> R1.2. Response actions, including roles and responsibilities of Cyber Security Incident response teams, Cyber Security Incident handling procedures, and communication plans.
>
> R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES-ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES-ISAC either directly or through an intermediary.
>
> R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.
>
> R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
>
> R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the Cyber Security Incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident. Testing the

Cyber Security Incident response plan does not require removing a component or system from service during the test.

CIP-008-2 R1 has a "Lower" VRF and a "High" VSL. This violation specifically addresses R1.4, which does not have an assigned VSL for the subrequirement level. Therefore, WECC made the determination of a "High" VSL based on R1.

URE submitted a Self-Report for a violation of CIP-008-2 R1. During its self-certification review of Version 1 of the Standard, URE found that its Cyber Security Incident response plan (Plan) was not updated to reflect the changes in Version 2 of the Standard. A few months later, WECC conducted an Audit of URE's facilities and reviewed URE's Self-Report and its compliance with Version 2 of the Standard. CIP-008-2 R1.4 requires that an entity's Plan address a process for updating the document within thirty calendar days of any changes. URE's Plan was not updated by the date the Version 2 Standard became mandatory and enforceable to reflect the change in the requirement from ninety days to thirty days.

WECC determined that URE was in violation of CIP-008-2 R1 because URE failed to update its Plan to reflect the change from ninety days to thirty days, per Version 2 of the Standard.

WECC determined the duration of the violation to be from the date the Version 2 Standard became mandatory and enforceable 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 because URE did not, during the period of the violation, have any changes to its Plan that needed to be updated; therefore URE did not fail to perform according to the Plan. However, URE did not revise its Plan to comply with the changes from Version 1 to Version 2. Therefore, the Plan set out an outdated response period. This violation only addresses R1.4. URE was in compliance with all other subrequirements of the Standard, dealing with the identification, classification, response and reporting of Cyber Security Incidents related to CCAs.

CIP-009-1 R1 (WECC201002349), CIP-009-1 R3 (WECC201002350)

The purpose statement of Reliability Standard CIP-009-1 provides: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
>
> R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
>
> R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R1 has a "Medium" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation. URE's recovery plan for CCAs failed to provide adequate information and define procedures to ensure a timely and effective recovery of CCAs after an event. Although URE stated that it has a documented recovery plan, WECC determined that URE did not create recovery plans for all CCAs, and there was limited correlation between CCAs and the available recovery procedures. URE's recovery plan process did not clearly specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plans. Further, its process did not clearly define the roles and responsibilities of responders.

WECC determined that URE was in violation of CIP-009-1 R1 because of its failure to create and annually review recovery plans for CCAs.

WECC determined the duration of the violation to be from the first day following Certification of Mitigation Plan Completion for a prior CIP violation of URE 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 because URE did have a recovery plan, despite the fact that the plan document did not clearly address all of the issues specified in the Standard.

CIP-009-1 R3 provides: "Change Control — Recovery plan(s) shall be updated to reflect any changes or lessons learned as a result of an exercise or the recovery from an actual incident. Updates shall be communicated to personnel responsible for the activation and implementation of the recovery plan(s) within ninety calendar days of the change."

CIP-009-1 R3 has a "Lower" VRF and a "Severe" VSL.

WECC notified URE that it was initiating the semi-annual CIP Self-Certification process. URE submitted a Self-Certification form certifying that although it was "substantially compliant," it was reporting a violation for the Self-Certification period. One week later, URE submitted a supplemental CIP Data Request Form with a detailed explanation and cause of the violation.

URE failed to update its recovery plans to reflect changes or lessons learned as a result of an exercise or the recovery from an actual incident. URE also failed to communicate updates to personnel responsible for the activation and implementation of its recovery plans within ninety calendar days of the change. URE has a written process for recovery plans, and during the review for Self-Certification, URE identified that there was a process for capturing lessons learned, but not for the implementation of lessons learned. URE discovered that the recovery plans were not updated for identified lessons learned, and URE had not communicated the lessons learned to the appropriate personnel.

WECC determined that URE was in violation of CIP-009-1 R3 because of its failure to update its recovery plans to reflect changes or lessons learned as a result of an exercise or the recovery from an actual incident, and to communicate updates to personnel responsible for the activation and implementation of the recovery plans.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE 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 because URE's recovery plan included a process for capturing lessons learned, although it could not provide documentation that those lessons were not communicated to its personnel within the thirty calendar days required by the Standard.

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 had an internal compliance program (ICP) in place at the time of the violations.
(2) URE's compliance 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 Plan[15]

CIP-003-1 R6 (WECC201002338)
URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on March 10, 2011 and approved by NERC on April 28, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on May 2, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its CIP-003-1 R6 change control and configuration management procedure;
2. Define and document a configuration management plan that defines all required configuration information;
3. Define what specifically constitutes a "significant change," and requires maintenance and tracking of identified configuration items in the procedure; and
4. Train affected personnel on the new plan and procedure.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. The change control and configuration management procedure;
2. The change control and configuration management plan; and
3. Training sign-in sheets as evidence of training.

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

[15] *See* 18 C.F.R § 39.7(d)(7).

CIP-004-1 R2 (WECC201002339)

URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 18, 2011 and approved by NERC on June 29, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 29, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Determine the key topics to include in its CIP training requirements;
2. Develop enhanced training materials;
3. Obtain management approval; and
4. Train its personnel (including the identified individual with access to CCAs who was not trained).

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

1. Updated training program; and
2. Evidence of training.

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

CIP-005-2 R1 (WECC201002361)

URE's Mitigation Plan to address its violation of CIP-005-2 R1 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 29, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop new ESP access procedures;
2. Reconfigure its network to remove all non-critical systems from within the ESP;
3. Reconfigure its network consistent with the new procedures; and
4. Incorporate the new procedures in URE's standard operating procedures.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan

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

1. CIP-005-3 R1 ESP inventory procedure;
2. CIP-005-3 R1 ESP dial-up access procedure;
3. CIP-005-3 R1 site configuration diagrams;
4. CIP-005-3 R1 ACM identification worksheet;
5. CIP-005-3 R1 ESP identification worksheet;
6. CIP-005-3 R1 non-CCA identification worksheet;
7. CIP-005 R1 review and training file;
8. Acceptance of responsibility form for the personnel responsible for the above procedures; and
9. Review and training sign in sheets.

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

CIP-005-2 R2 (WECC201002362)

URE's Mitigation Plan to address its violation of CIP-005-2 R2 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 29, 2011 and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop an electronic access control procedure for securing dial-up connections;
2. Develop related procedures, worksheets and forms that document organizational processes and technical and procedural mechanisms; and
3. Train personnel.

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

1. CIP-005-3 R2 access point and access control documentation form and CIP-005-3 R2 access point banner text documentation form;
2. CIP-005-3 R1 ESP dial-up access procedure;

3. CIP-005-3 R2.2 access point authorized ports and services procedure;
4. CIP-005-3 R2 access point authorized ports and services list; and
5. CIP-005 procedures evidence review and training and CIP-005 R2 review and training documents.

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

CIP-005-2 R3 (WECC201002363)

URE's Mitigation Plan to address its violation of CIP-005-2 R3 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 29, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement clear review and documentation processes for its monitoring and logging access procedures and train employees on log review requirements; and
2. Order new servers which can better screen and alert on important security events, and incorporate these devices into its remediation plan.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. CIP-005-3 electronic access point monitoring procedure;
2. The security event management system plan;
3. CIP-005-3 R3 access point access alerting documentation form;
4. CIP-005-3 R3 ESP alert log;
5. Acceptance of responsibility form for the personnel responsible for the above procedure;
6. CIP-005 R3 review and training sign-in sheets; and
7. CIP-005 R3 security event management system training overview and sign-in sheet.

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

CIP-005-2 R4 (WECC201002364)

URE's Mitigation Plan to address its violation of CIP-005-2 R4 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 29, 2011 and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Create and implement cyber vulnerability assessment procedures; and
2. Train URE personnel.

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

1. ESP vulnerability assessment procedures; and
2. CIP-005 R4 training and attendance information.

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

CIP-007-1 R1 (WECC201002341)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 29, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop cyber security testing change control procedures approved by URE management; and
2. Train URE personnel.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. CIP-007-3 R1 testing security controls for changes to existing firmware-based Cyber Assets procedure;

2. CIP-007-3 R1 testing security controls for changes to existing operating system-based Cyber Assets procedure;
3. CIP-007-3 R1 testing security controls for new firmware-based Cyber Assets procedure;
4. CIP-007-3 R1 testing security controls for new operating system-based Cyber Assets procedure;
5. Site configuration diagram;
6. CIP-003-3 R6 change control log extract;
7. CIP-007-3 R1 testing procedure checklists;
8. CIP-007 R1 review and training documentation;
9. Acceptance of responsibility forms for the personnel responsible for the cyber security testing change control procedures; and
10. Sign-in sheet for the training of personnel responsible for the procedures.

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

CIP-007-1 R3 (WECC201002342)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 2, 2011, and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop a security patch management procedure approved by URE management; and
2. Train URE personnel.

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

1. Revisions of the security patch tracking log;
2. Revisions of the security patch documentation form; and
3. Sign-in sheet for the training of personnel responsible for the procedure.

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

CIP-007-1 R4 (WECC201002343)

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 11, 2011 and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify all systems that require anti-malware solutions, then document these systems and implement procedures designed to ensure the systems are properly managed and controlled, and obtain management approval; and
2. Train the appropriate personnel.

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

1. Nine review procedures that comply with CIP-007 R9;
2. Annual review worksheets for account management documentation, disposal or redeployment documentation, malicious software prevention documentation, ports and services documentation, security controls test documentation, security patch management documentation, security status monitoring documentation, and system management and vulnerability assessment documentation;
3. Sign-in sheet for the training of personnel responsible for the above procedures; and
4. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the procedures, which indicate that they understand the procedure requirements.

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

CIP-007-1 R5 (WECC201002344)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 3, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its procedures for administrative shared accounts, password changes and account management, and obtain management approval; and
2. Train the appropriate personnel.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. User account activity documentation;
2. CIP-007-3 R5 user account access logging procedure;
3. Changing shared administrator account passwords spreadsheet;
4. CIP-007-3 R5 shared accounts list;
5. CIP-007-3 R5 EMS shared accounts list;
6. CIP-007-3 R5 administrator account management procedure;
7. CIP-007-3 R5 factory default accounts procedure;
8. CIP-007-3 R5 password management procedure;
9. CIP-007-3 R5 shared account management procedure;
10. CIP-007-3 R5 user account accessing logging procedure;
11. CIP-005 R3 security event management system training overview;
12. CIP-005 R3 security event management system plan training sign-in documentation;
13. CIP-007 R5 review and training documentation;
14. Acceptance of responsibility form for the personnel responsible for the above procedures; and
15. CIP review and training sign-in sheets.

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

CIP-007-1 R6 (WECC201002345)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 4, 2011 and approved by NERC on June 13,

2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Draft a new security status monitoring tool, revise its CIP-007 R6 cybersecurity event procedure and obtain management approval; and
2. Train appropriate personnel.

URE requested an extension of time to complete the mitigation activities. WECC approved URE's extension request and granted the extension. URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the following:

1. URE's CIP-007-3 R6 cybersecurity event procedure;
2. Screenshots of alerts from the security event management system;
3. Sample event logs from the security event management system security device;
4. Screenshots showing logs were retained for 6 months;
5. Security event management system report log and CIP-005-3 R3 ESP alert log;
6. CIP-007-3 R6 manual security event log review form; and
7. Training roster and responsibility forms for the new cybersecurity event procedure.

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

CIP-007-1 R7 (WECC201002346)

URE's Mitigation Plan to address its violation of CIP-007-1 R7 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 4, 2011 and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its CIP-007 R7 procedure to develop, implement and train personnel in disposal and redeployment methods, processes and procedures, and to obtain management approval; and
2. Train the appropriate personnel.

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

1. Disposal or redeployment procedure that complies with CIP-007 R7;
2. Electronic media redeployment form;
3. Sign-in sheet for the training of personnel responsible for this procedure; and
4. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the procedure, indicating that they understand the procedure requirements.

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

CIP-007-1 R8 (WECC201002347)

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 17, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revise its CIP-007 R8 procedure related to the cyber vulnerability assessment process and obtain management approval;
2. Train the appropriate personnel; and
3. Perform a vulnerability assessment.

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

1. CIP-007-3 R8 cyber vulnerability assessment procedure;
2. CIP-007-3 R8 cyber vulnerability assessment worksheet;
3. CIP-007-3 R2 authorized physical ports documentation (16 files);
4. CIP-007-3 R5 EMS administrator and default account review log;
5. CIP-007 R8 review and training documentation and training sign-in sheet; and
6. Acceptance of responsibility form for the personnel responsible for the procedure.

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

CIP-007-1 R9 (WECC201002348)

URE's Mitigation Plan to address its violation of CIP-007-1 R9 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 5, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement a CIP-007 document review and maintenance procedure to clearly define the review process and obtain management approval; and
2. Train the appropriate staff and implement review procedures to ensure all necessary documents are appropriately reviewed within the necessary timeframe.

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

1. Nine review procedures that address CIP-007 R9;
2. Annual review worksheets for account management documentation, disposal, or redeployment documentation, malicious software prevention documentation, ports and services documentation, security controls test documentation, security patch management documentation, security status monitoring documentation, system management and vulnerability assessment documentation;
3. Sign-in sheet for the training of personnel responsible for this procedure; and
4. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the CIP-007 procedures, indicating that they understand the procedure requirements.

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

CIP-008-2 R1 (WECC201002365)

URE's Mitigation Plan to address its violation of CIP-008-2 R1 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on April 27, 2011 and approved by NERC on June 10, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 10, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update its Plan to reflect Version 2 of the Standard; specifically, changing the update requirement from ninety days to thirty days;
2. Review CIP-008 R1.5 and R1.6 and include processes for annual review and testing of the Plan; and
3. Train the applicable personnel.

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

1. Updated Plan that complies with CIP-008 R1;
2. Cyber Security Incident classification procedure and Cyber Security Incident reporting process documents, the purpose of which is to ensure the identification, classification response, communication and reporting of Cyber Security Incidents related to CCAs, non-CAs inside the ESP and ACMs;
3. Incident response exercise and drill documents;
4. Sign-in sheet for the training of personnel responsible for this procedure; and
5. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the procedure, indicating that they understand the procedure requirements.

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

CIP-009-1 R1 (WECC201002349)

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 10, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Draft a new recovery plan that directly addresses all CCAs, defines roles and responsibilities of responders, and specifies the required response actions by varying duration and severity that clearly meets the CIP-009 R1 Standard; and
2. Train stakeholders on the recovery plan and implement it.

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

1. Updated recovery plan documents, the purpose of which is to restore CCAs and ACM devices to operation condition in the event of an incident;
2. Cyber Asset recovery plan roles assignments list and its backup information form;
3. Sign-in sheet for the training of personnel responsible for this procedure; and
4. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the procedure, indicating that they understand the procedure requirements.

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

CIP-009-1 R3 (WECC201002350)

URE's Mitigation Plan to address its violation of CIP-009-1 R3 was submitted to WECC on November 17, 2010. The Mitigation Plan was accepted by WECC on May 10, 2011 and approved by NERC on June 13, 2011. The Mitigation Plan for this violation was submitted as non-public information to FERC on June 17, 2011 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement and document a recovery plan lessons-learned process; and
2. Begin using the lessons learned to strengthen existing recovery plans.

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

1. Updated recovery plan documents and exercise sign-in sheet, which demonstrate that the updated CCA recovery plan procedure has a method of documenting annual exercises and incorporating lessons learned when needed;
2. Sign-in sheet for the training of personnel responsible for this procedure; and
3. Acceptance of responsibility forms for the individuals that are responsible for the roles listed in the procedure, indicating that they understand the procedure requirements.

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 August 14, 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 compliance history;
2. WECC reported that URE was cooperative throughout the compliance enforcement process;
3. URE had an ICP at the time of the violations which WECC considered a mitigating factor;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
6. 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 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.

[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).

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.

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;

b) Addendum No. 1 to the Settlement Agreement by and between WECC and URE;

c) Self-Certification covering violations of WECC201002338 CIP-003-1 R6, WECC201002339 CIP-004-1 R2, WECC201002361 CIP-005-2 R1, WECC201002362 CIP-005-2 R2, WECC201002363 CIP-005-2 R3, WECC201002364 CIP-005-2 R4, WECC201002341 CIP-007-1 R1, WECC201002342 CIP-007-1 R3, WECC201002343 CIP-007-1 R4, WECC201002345 CIP-007-1 R6, WECC201002346 CIP-007-1 R7, WECC201002347 CIP-007-1 R8, WECC201002348 CIP-007-1 R9, WECC201002349 CIP-009-1 R1, and WECC201002350 CIP-009-1 R3;

d) Record documents for WECC201002338 CIP-003-1 R6:

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

e) Record documents for WECC201002339 CIP-004-1 R2:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

f) Record documents for WECC201002361 CIP-005-2 R1:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

g) Record documents for WECC201002362 CIP-005-2 R2:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

h) Record documents for WECC201002363 CIP-005-2 R3:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

i) Record documents for WECC201002364 CIP-005-2 R4:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

j) Record documents for WECC201002341 CIP-007-1 R1:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

k) Record documents for WECC201002342 CIP-007-1 R3:

1) URE's Mitigation Plan;

2) URE's Certification of Mitigation Plan Completion;

3) WECC's Verification of Mitigation Plan Completion;

l) Record documents for WECC201002343 CIP-007-1 R4:

1) URE's Mitigation Plan;

2) URE's Certification of Mitigation Plan Completion;

3) WECC's Verification of Mitigation Plan Completion;

m) Record documents for WECC201002344 CIP-007-1 R5:

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;

n) Record documents for WECC201002345 CIP-007-1 R6:

1) URE's Mitigation Plan;

2) URE's Certification of Mitigation Plan Completion;

3) WECC's Verification of Mitigation Plan Completion;

o) Record documents for WECC201002346 CIP-007-1 R7:

1) URE's Mitigation Plan;

2) URE's Certification of Mitigation Plan Completion;

3) WECC's Verification of Mitigation Plan Completion;

p) Record documents for WECC201002347 CIP-007-1 R8:

1) URE's Mitigation Plan;

2) URE's Certification of Mitigation Plan Completion;

3) WECC's Verification of Mitigation Plan Completion;

q) Record documents for WECC201002348 CIP-007-1 R9:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

r) Record documents for WECC201002365 CIP-008-2 R1:
   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;

s) Record documents for WECC201002349 CIP-009-1 R1:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion;
   3) WECC's Verification of Mitigation Plan Completion;

t) Record documents for WECC201002350 CIP-009-1 R3:
   1) URE's Mitigation Plan;
   2) URE's Certification of Mitigation Plan Completion; and
   3) 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 u.

[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 Sandy Mooy* Associate General Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7658 (801) 883-6894 – facsimile SMooy@wecc.biz Christopher Luras* Director of Compliance Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

NERC respectfully requests that the Commission accept this Notice of Penalty as compliant with its rules, regulations and orders.

Respectfully submitted,

/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