PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 30, 2013

Ms. Kimberly D. Bose
Secretary
Federal Energy Regulatory Commission
888 First Street, N.E.
Washington, DC 20426

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP13-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations and orders, as well as NERC 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 the 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-002-1 R3; CIP-003-2 R1.2,[4] R3, R4, and R5; CIP-004-1 R2 and R4; CIP-005-1 R1; CIP-006-1 R1; CIP-007-1 R1, R2, R3, R5, R6, R8, and R9; and CIP-009-1 R5. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed

[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] This violation involves Version 2 and Version 3 of this CIP Standard. The Settlement Agreement incorrectly states that the violation involved Version 1 of the Standard. The remaining violations in this Full Notice of Penalty also include several Versions of this Standard, starting with Version 1. For ease of reference, this Full Notice of Penalty refers to CIP-003-2 R1 and to Version 1 of the remaining violations.

penalty of two hundred ninety-one thousand dollars ($291,000), 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 WECC201102568, WECC201102569, WECC201102582, WECC201102581, WECC201102587, WECC201102589, WECC201102591, WECC201102574, WECC201102596, WECC201102578, WECC201102579, WECC201102580, WECC201002549, WECC201102592, WECC201102837, WECC201102550, and WECC201102556 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 March 5, 2012 by and between WECC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-1290	WECC201102568	CIP-002-1	R3	High	$291,000
			WECC201102569	CIP-003-2	R1.2	Lower	
			WECC201102582	CIP-003-1	R3	Lower	
			WECC201102581	CIP-003-1	R4	Lower	
			WECC201102587	CIP-003-1	R5	Lower	
			WECC201102589	CIP-004-1	R2	Medium	
			WECC201102591	CIP-004-1	R4	Lower	
			WECC201102574	CIP-005-1	R1	Medium	
			WECC201102596	CIP-006-1	R1	Medium	
			WECC201102578	CIP-007-1	R1	Medium	
			WECC201102579	CIP-007-1	R2	Medium	
			WECC201102580	CIP-007-1	R3	Lower	

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
			WECC201002549	CIP-007-1	R5	Medium	
			WECC201102592	CIP-007-1	R6	Medium	
			WECC201102837	CIP-007-1	R8	Lower	
			WECC201102550	CIP-007-1	R9	Lower	
			WECC201102556	CIP-009-1	R5	Lower	

CIP-002-1 R3 (WECC201102568)

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

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.
>
> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at

control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time inter utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

R3.3. The Cyber Asset is dial-up accessible.

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

WECC issued a Notice of Self-Certification to URE. URE submitted its Self-Certification citing noncompliance with CIP-002-1 R3 and CIP-005-3 R3. URE reported that it failed to update as necessary the Critical Cyber Assets (CCAs) list for its generating station, in violation of CIP-002-1 R3.

WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Compliance Audit (Audit), WECC's Audit Team reviewed URE's compliance with CIP-002-1 R3 and URE's Self-Certification. Based on its review of the Self-Certification and on-site investigation, the Audit Team determined that URE failed to update as necessary its CCA list associated with URE's generating station.

The Audit Team identified two CCAs on URE's CCA list that were removed from service and 14 CCAs that were removed from service two months later. These CCAs remained on the list more than a year later. In total, the Audit Team determined that URE failed to remove 16 CCAs from the CCA list at URE's generating station, in violation of CIP-002-1 R3.

In addition, the scope of this violation includes Audit Team findings that expanded beyond the URE noncompliance cited by URE in its Self-Certification. The Audit Team conducted an on-site inspection of URE's generating station and identified dial-up accessible CCAs associated with

URE's generating station's automatic voltage regulator (AVR). The Audit Team determined that URE's failure to identify this dial-up Cyber Asset as a CCA violated CIP-002-1 R3.

WECC Enforcement (Enforcement) reviewed the record and determined that URE failed to update its CCA list as necessary and remove 16 CCAs from its CCA list. WECC Enforcement also determined that the scope of URE noncompliance included its failure to identify a dial-up accessible CCA associated with URE's generating station. Although the CCA may have been used intermittently, the device constituted a dial-up accessible CCA essential to the operation of URE's generating station, as a Critical Asset. Evidence from the on-site Audit suggests that the device remained connected as of the fall of 2010. Enforcement therefore determined that URE was required to identify the CCA as of the date by which it was required to reach compliance with this Standard.

WECC determined that URE violated CIP-002-1 R3 because URE failed to identify all CCAs associated with its generating station and failed to update its CCA list for the same generating station as necessary.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). First, URE demonstrated that the scope of the violation was limited to the CCA list maintained at URE's generating station and did not include CCA lists maintained for its control center, thus reducing the risk to the BPS. Second, WECC determined that URE's failure to update the CCA list resulted in unnecessary inclusion of 16 CCAs that were decommissioned during the first quarter of 2010. Because URE's list was over-inclusive, rather than under-inclusive, WECC determined that the risk to the BPS from this instance of noncompliance was minimal. Third, the risk to the BPS presented by URE's failure to identify a single dial-up device as a CCA was mitigated by the fact that the device had limited dial-up connectivity. Finally, the physical and electronic access to the CCAs was controlled and monitored by URE.

CIP-003-2 R1.2 (WECC201102569)

The purpose statement of Reliability Standard CIP-003-2 provides: "Standard CIP-003-2 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-2 should be read as part of a group of standards numbered Standards CIP-002-2 through CIP-009-2."

CIP-003-2 R1 provides in pertinent part:

> R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> ***
>
> R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

CIP-003-2 R1.2 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification, citing noncompliance with CIP-003-2 R1. URE reported that it failed to ensure that its cybersecurity policy (Policy) was readily available to all personnel who have access to, or are responsible for, CCAs at URE's generating station.

WECC's subject matter expert (SME) reviewed the Self-Certification and determined that URE was in violation of R1.2. Although URE made its Policy available on its intranet site, it did not make hard copies available to personnel, including contractors, without access to URE's intranet. As a result, 60 individuals were not able to access URE's Policy.

WECC Enforcement reviewed the record and determined that URE violated CIP-003-2 R1.2 because URE failed to make its Policy available to all personnel with access to CCAs at URE's generating station.

WECC determined the duration of the violation to be from the first date after URE mitigated a prior violation of this Standard, through the date 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. Although URE failed to make its Policy available to individuals without access to its intranet site, URE did initially provide on-site employees with a copy of the Policy during cybersecurity training sessions. Also, the scope of the violation was limited to 60 individuals with limited physical access to CCAs at URE's generating station. WECC also determined that although these individuals did not have access to electronic or hard copies of

the policy, URE management at URE's generating station discussed URE's Policy updates and reinforced compliance with the Policy at URE's weekly staff meetings.[5]

CIP-003-1 R3 (WECC201102582)

CIP-003-1 R3 provides:

> R.3. Exceptions — Instances where the Responsible Entity cannot conform to its cyber security policy must be documented as exceptions and authorized by the senior manager or delegate(s).
>
> > R3.1. Exceptions to the Responsible Entity's cyber security policy must be documented within thirty days of being approved by the senior manager or delegate(s).
> >
> > R3.2. Documented exceptions to the cyber security policy must include an explanation as to why the exception is necessary and any compensating measures.
> >
> > R3.3. Authorized exceptions to the cyber security policy must be reviewed and approved annually by the senior manager or delegate(s) to ensure the exceptions are still required and valid. Such review and approval shall be documented.

CIP-003-1 R3 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification citing noncompliance with CIP-003-1 R3. URE reported that it failed to document all Policy exceptions at URE's generating station or to include an explanation as to why exceptions at URE's generating station were necessary.

URE submitted a Self-Report that expanded the scope of CIP-003-1 R3.[6] URE reported that in 2010 it failed to review annually documented exceptions to its Policy at its control center.

[5] No information explaining exactly which employees participated in the staff meetings was made available.
[6] WECC consolidated the noncompliance reported in the Self-Report and in the Self-Certification under the same violation ID: WECC201102582. WECC determined that Self-Certification was the appropriate method of discovery.

WECC reviewed the Self-Certification submitted by URE and determined that there was one exception to URE's Policy which required documentation under CIP-003 R3. The exception stems from delayed implementation of URE's personnel risk assessment (PRA) program. URE's Policy requires individuals to complete CIP-004 R2 training prior to receiving access to CCAs. Approximately 243 individuals with access to CCAs at URE's generating station are represented by the International Brotherhood of Electrical Workers (IBEW) and are subject to the terms of a bargaining unit agreement that precludes URE from conducting criminal background checks for these employees. Due to delayed negotiations with the IBEW, URE was unable to implement its PRA program with respect to these employees. URE did not revoke access to these employees and, instead, exempted them from its PRA program until the bargaining unit agreement was revised with terms allowing URE to conduct criminal background checks.

WECC determined that URE violated CIP-003-1 R3 because URE failed to document one exemption from its PRA program applicable to URE's generating station.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. Although URE failed to document one exception to its Policy at the URE's generating station, it documented exceptions to its Policy pertaining to its control center. Also, although URE failed to review all documented exceptions to its Policy in 2010, it conducted annual reviews in 2009 and 2011.

CIP-003-1 R4 (WECC201102581)

CIP-003-1 R4 provides:

> R4. Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
>
> > R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP- 002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.

R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.

R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

CIP-003-1 R4 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification citing noncompliance with CIP-003-3 R4. Specifically, URE reported that it failed to protect its cyber incident response plans pursuant to CIP-003-1 R4.1. Further, URE failed to assess adherence to its information protection program (IPP), it failed to protect CCA information described under R4.1, and failed to assess annually its adherence to its IPP.

WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Audit, WECC's Audit Team reviewed URE's compliance with CIP-003-1 R4, including URE's Self-Certification. WECC SMEs determined that the IPP in place at URE's generating station did not include printed documentation located at the facility, in violation of R4.1. Furthermore, the Audit Team determined that URE failed to identify and designate consistently CCA information to be protected, as required by R4.2. Lastly, the Audit Team determined that URE failed to assess annually its adherence to its Policy, as required by R4.3.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-003-1 R4 because it failed to: implement its IPP at URE's generating station as of January 1, 2010; protect information under R4.1; classify information under R4.2; and annually review its IPP and assess adherence thereto under R4.3, for 2009 and 2010.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. URE had an IPP during the pendency of the violation, and the IPP was implemented at the control center and backup control center. URE regularly conducted on-site staff meetings that included discussion of information protection procedures, as cited in its Policy. Finally, the scope of URE's violation was limited to CCAs at URE's generating station.

CIP-003-1 R5 (WECC201102587)

CIP-003-1 R5 provides:

> R5: Access Control- The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> R5.1 The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>
> R5.1.1. Personnel shall be identified by name, title, and the information for which they are responsible for authorizing access.
>
> R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
>
> R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
>
> R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

CIP-003-1 R5 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted its Self-Certification, citing noncompliance with CIP-003-1 R5. Specifically, URE reported that although it had a documented program for managing access to protected CCA information, URE failed to implement that program at URE's generating station.

On March 2, 2011, WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Audit, WECC audited URE for compliance with CIP-003-1 R5, including the noncompliance cited in URE's Self-Certification. The Audit Team determined that URE failed to demonstrate that it managed access to protected information that was physically located at URE's generating station. Furthermore, the Audit Team determined that URE failed to maintain a list of designated personnel responsible for authorizing logical or physical access to protected

information. Also, in 2009, URE failed to assess its process for controlling access privileges to protected information.

Enforcement reviewed the record and determined that URE had a violation of CIP-003-1 R5 because it failed to: document and implement a program for managing access to protected CCA information; maintain a list of designated personnel responsible for authorizing logical or physical access to protected information; and assess its process for controlling access privileges to protected information.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. URE did document a process to manage protected information for CCAs housed at its control center. Although URE failed to implement the process at URE's generating station, URE regularly conducted on-site staff meetings that included information protection procedures, as cited in its Policy. Also, the scope of URE's violation was limited to access management to CCA information at the URE's generating station.

CIP-004-1 R2 (WECC201102589)

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 has a "Medium" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted its Self-Certification citing noncompliance with CIP-004-1 R2. Specifically, URE reported that it failed to ensure that individuals with access to CCAs at URE's generating station completed training within 30 days of being granted access to CCAs, in violation of CIP-004-1 R2. Furthermore, URE reported noncompliance with R2.2 because its training program did not address R2.2.1 and R2.2.4; and URE also reported noncompliance for failing to maintain documentation demonstrating annual training was completed as required by R2.3. URE submitted a Self-Report that expanded the scope of the noncompliance, adding to the violation of R2.3 initially disclosed in its Self-Certification. In its Self-Report, URE disclosed that two individuals did not receive annual training in 2010.

WECC issued a Notice of On-site Compliance Audit to URE. WECC audited URE compliance with CIP-004-1, including URE's Self-Certification and Self-Report. The Audit Team reviewed training logs and records, and determined that approximately 120 individuals received access to CCAs without completing training per the timeline prescribed under R2. The Audit Team also reviewed URE's training program documentation and determined that URE's training failed to address R2.2.1 and R2.2.4. The Audit Team determined that the scope of URE's noncompliance with R2.2 was limited to the training program implemented for individuals with access to CCAs

at URE's generating station. Lastly, the Audit Team confirmed that two individuals did not receive annual retraining, in violation of CIP-004-1 R2.3.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-004-1 R2 because it granted 312 individuals physical access to CCAs at URE's generating station. Because URE's training was limited by an existing collective bargaining agreement, approximately 120 represented individuals failed to complete training within 90 days of being granted access to CCAs at URE's generating station.[7] Enforcement also determined that approximately 48 contractors granted access to CCAs received limited training that did not address the requirements of R2.2.1 and R2.2.4. Finally, Enforcement determined that approximately two individuals did not complete annual training in 2010 pursuant to R2.3.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, although URE failed to ensure that individuals completed training as required by this Standard, URE regularly conducted on-site staff meetings that included information covered in URE's training program. The risk was mitigated by the fact that the individuals at issue had PRAs and had been granted unescorted physical access to the CCAs at URE's generating station. Furthermore, these individuals did not have electronic access to CCAs at URE's generating station. The scope of the violation did not include individuals with access to CCAs at URE's control center, who completed training pursuant to CIP-004-1 R2.

CIP-004-1 R4 (WECC201102591)

CIP-004-1 R4 provides:

> R4. Access - The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.

[7] CIP-004-1 R2 (effective July 1, 2008 to March 31, 2010) mandated training within 90 days of receiving access to CCAs. As of April 1, 2010, subsequent versions of the Standard, CIP-004-2 and CIP-004-3, mandated training prior to being granted access to CCAs.

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification citing noncompliance with CIP-004-1 R4. Specifically, URE reported that it failed to maintain lists that included specific electronic and physical access rights granted to personnel at URE's generating station. Furthermore, URE reported that it failed to revoke access rights within the timeframe prescribed under R4.2 at URE's generating station.

WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Audit, WECC assessed URE compliance with CIP-004-1 R4 and reviewed the Self-Certification. The Audit Team reviewed documentation detailing maintenance and controls for lists of personnel with access to CCAs at URE's generating station.

The Audit Team determined that URE failed to maintain access lists that included specific access rights, in violation of CIP-004-1 R4. Furthermore, the Audit determined that URE failed to review its access lists quarterly and failed to update access lists at URE's generating station to reflect changes in personnel or changes in access rights.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-004-1 R4 because URE failed to: maintain lists that included specific access rights; update its lists within seven calendar days of a change in personnel; review its access lists quarterly; and revoke access for personnel who no longer require such access.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. Although URE failed to review and maintain its lists of personnel with authorized access to CCAs at URE's generating station, URE created and maintained access lists for access granted to CCAs associated with its control center. URE also demonstrated that although lists maintained at URE's generating station did not identify specific access rights, the lists did identify individuals with physical access to the CCAs. Furthermore, both facilities have layered physical security, which requires individuals to present credentials and sign a login sheet before entering either the control center or URE's generating station.

CIP-005-1 R1 (WECC201102574)

The purpose statement of Reliability Standard CIP-005-1 provides: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 provides:

> R.1. 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.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

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

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification, citing noncompliance with CIP-005-1 R1. Specifically, URE reported that it failed to identify three firewalls as access points to the URE's generating station Electronic Security Perimeter (ESP).

WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Audit, WECC assessed URE's compliance with CIP-005-1 and reviewed URE's Self-Certification. The Audit Team reviewed URE's ESP diagrams and CCA lists. The Audit Team confirmed that URE failed to identify three firewalls as access points to the URE's generating station ESP, in violation of CIP-005-1 R1.1. Enforcement reviewed the record and determined that URE had a violation of CIP-005-1 R1 for a failure to identify three firewalls as ESP access points. Enforcement determined that URE also established an ESP at its control center, but ESP access points for this facility appeared to be identified and secured.

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. URE implemented layered security systems in front of the CCAs at issue during the violation period. Access to the three firewalls was granted through a secured, corporate network. Additionally, each firewall was password-protected. Access to the devices was limited to 28 individuals using one of three shared management accounts. Once a user gained access through any one of the firewalls, that user had limited access to a subset of Cyber Assets within the ESP.

CIP-006-1 R1 (WECC201102596)

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

CIP-006-1 R1 provides:

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

R1. Physical Security Plan — The Responsible Entity[8] shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

[8] Within the text of Standard CIP-006 "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

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

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

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

WECC issued a Notice of Self-Certification to URE. URE submitted a Self-Certification, citing noncompliance with CIP-006-1 R1. Specifically, URE reported that it failed to ensure that all Cyber Assets resided within a Physical Security Perimeter (PSP). URE disclosed that it did not document and implement a visitor control program as required by R1.6, and that it failed to afford all protective measures prescribed under R1.8 to Cyber Assets provisioning physical access control and monitoring at URE's generating station.

WECC issued a Notice of On-site Compliance Audit to URE. During the course of the Audit, the Auditors assessed URE's compliance with CIP-006-1, including URE's Self-Certification. Based on the Audit Team's review of the Self-Certification and inspection of URE PSPs, the Auditors determined that URE was in violation of CIP-006-1 R1 for its failure to demonstrate compliance with R1.1 and R1.8.

Specifically, the Audit Team determined that two PSPs at the URE's generating station facility did not constitute a "six-wall" border pursuant to R1.1. The Audit Team identified three holes in the URE's generating station distributed control system (DCS) shop PSP.[9] The Audit team

[9] "Shop" refers to the area located within the DCS.

identified: 1) a 20' x 25' drop ceiling in the DCS shop PSP; 2) a 3' x 3' hole adjacent to heating, ventilation, and air conditioning (HVAC) venting in the DCS shop PSP; and 3) a vent that could be manually opened to provide ingress but not egress from the DCS. Furthermore, the Audit Team identified a breach in an unsecured door that opened to a 16-foot drop to the control room floor in the URE's generating station control room PSP. Although the door did not provide immediate access to the control room, given the 16-foot drop to the control room floor, the 7' x 3' doorway was not secured and therefore constituted a breach in URE's PSP at URE's generating station.

Furthermore, the Audit Team also determined that URE failed to ensure that three devices provisioning PSP access control were secured pursuant to CIP-006-1 R1.8. The Audit Team identified two control panels in URE's control center not secured pursuant to R1.8. The third Cyber Asset within scope of this noncompliance was a workstation used to manage access control and monitoring for PSPs at URE's generating station. Consistent with URE's Self-Certification, the Audit Team determined that URE failed to implement all protective measures prescribed under CIP-006-1 R1.8. The Audit Team determined that URE failed to implement malicious software prevention measures described under CIP-007-1 R4 and applicable to PSP access control and monitoring devices, as required by CIP-006-1 R1.8. The Audit Team determined that URE was in violation of CIP-006-1 R1.1 and R1.8 and forwarded its findings to WECC Enforcement.

WECC determined that URE had a violation of CIP-006-1 R1.1 and 1.8 because it failed to identify all PSP access points and secure three Cyber Assets provisioning physical access control and monitoring pursuant to CIP-006-1 R1.8.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The identified access points were equipped at all times with alarming and monitoring equipment. Both the control center and URE's generating station are continuously remotely monitored by on-site security staff. Furthermore, both facilities have layered physical security, which requires individuals to present credentials and sign a login sheet before entering either the control center or URE's generating station.

CIP-007-1 R1 (WECC201102578)

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 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 cybersecurity 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 issued a Notice of Self-Certification to URE. URE submitted its Self-Certification citing noncompliance with CIP-007 R1.1, R1.2, and R1.3. Specifically, URE reported that it failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets or CCAs within ESPs do not negatively impact existing security controls.

WECC conducted an on-site Audit of URE. The Audit Team reviewed URE's Self-Certification and audited URE for CIP-007-1 R1 compliance. The Audit Team determined that URE was in violation of CIP-007-1 R1 and its sub-requirements.

Specifically, URE established a single ESP for 88 CCAs and 300 Cyber Assets associated with URE's generating station.[10] The Audit Team reviewed URE testing procedures for CIP-007-1 R1, including revised testing procedures addressing ClP-007-1 R1. The Auditors determined that URE failed to create and implement testing procedures that minimized adverse effects on the production environment. The Auditors found that URE's testing procedures addressed functionality testing, to ensure significant changes did not negatively impact system operations. However, with respect to security tests, the Audit Team determined that URE's testing procedure did not require assessment of the impact of significant changes to ESP security. The Audit Team therefore determined that URE was in violation of R1.1.

The Audit Team also determined that URE was in violation of CIP-007-1 R1.2 because it failed to provide documentation of testing in a manner that reflects the production environment. The Audit Team reviewed URE documentation addressing CIP-007 R1.2. The Audit Team determined that testing documentation for CCAs and Cyber Assets within the ESP at URE's generating station did not document how testing was performed and how testing impacts the existing ESP security controls. Furthermore, URE failed to provide evidence of any test results, in violation of R1.3.

Based on the Audit Team's review and investigation of URE compliance with CIP-007 R3, the Audit Team determined that URE failed to reach compliance with CIP-007-1 R1 as of the date the Standard became mandatory and enforceable for URE.

The Audit Team forwarded its findings to WECC Enforcement, which reviewed the record and determined that URE failed to comply with CIP-007-1 R1 because it did not ensure that its testing procedure included assessment of the impact of significant changes to ESP security, and because it failed to conduct testing in a manner that reflects the production environment.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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 failed to assess significant changes to security of ESPs at URE's generating station. However, the scope of the violation is limited to one ESP. Within the ESP, URE created clusters of Cyber Assets within mini ESPs, which were

[10] As described in the violation of CIP-002-1 R3 above, URE failed to identify all CCAs associated with the Critical Asset.

protected by additional firewalls and passwords. Therefore, penetration of the ESP through the energy management system (EMS) would not expose all Cyber Assets within the ESP to attack or misuse. Further, the entire ESP is secured behind URE's corporate local area network (LAN), whereby users must first access the corporate intranet site from a URE facility before attempting to access the URE's generating station ESP. The corporate LAN is an isolated network that also requires specific credentials and passwords for access.

CIP-007-1 R2 (WECC201102579)

CIP-007-1 R2 provides:

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

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

WECC issued a Notice of Self-Certification to URE. URE submitted its Self-Certification, citing noncompliance with CIP-007-3 R2. Specifically, URE reported that it failed to document and implement a process to ensure only ports and services required for normal and emergency operations are enabled, in violation of CIP-007-1 R2.1, R2.2, and R2.3.

WECC issued a Notice of On-site Compliance Audit to URE. The Audit Team assessed URE's compliance with CIP-007-3 R2, including URE's Self-Certification. After visual inspection of URE facilities and CCAs within the control center and URE's generating station, the Audit Team determined that URE failed to ensure that only ports and services required for normal and

emergency operations were enabled. The Audit Team determined that URE was in violation with CIP-007-1 R2 and forwarded its findings to WECC Enforcement.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-007-1 R2.2 because it failed to enable only those ports and services required for normal and emergency operations. WECC determined that the scope of the violation included URE's control center and its generating station. Enforcement determined that URE failed to disable other ports and services prior to deploying its EMS.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, although URE failed to enable only those ports and services required for normal and emergency operations, physical access to URE's Cyber Assets and ports and services was limited. URE secured Cyber Assets within perimeters to which access was controlled and monitored. Further, employees with physical and logical access were briefed on ports and service use in the course of employee training and weekly staff meetings with URE management.

CIP-007-1 R3 (WECC201102580)

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 issued a Notice of Self-Certification to URE. URE submitted its Self-Certification, citing noncompliance with CIP-007-3 R3. Specifically, URE failed to document and implement a security patch management program for Cyber Assets at URE's generating station. URE also reported that for a subset of Cyber Assets in its EMS system, URE did not assess security patches within thirty days of availability, in violation of R3.1. URE also failed to document its assessment of security patches available for EMS Cyber Assets, in violation of R3.2.

WECC issued a Notice of On-site Compliance Audit to URE. The Audit Team assessed URE compliance with CIP-007-3 R3, including URE's Self-Certification, and determined that although URE documented and implemented a security patch management program at its control center, URE failed to implement that program with respect to Cyber Assets within URE's EMS. Furthermore, the Audit Team determined that URE failed to document or implement a security patch management program for Cyber Assets associated with URE's generating station. URE did not include the vendor testing in its security patch management program for URE's generating station. Although the devices were being tested by the vendor, URE did not reflect this work in its program.

The Audit Team, therefore, determined that URE was in violation of CIP-007-1 R3 and forwarded its findings to WECC Enforcement.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-007-1 R3 because it documented a security patch management program but failed to implement it with respect to Cyber Assets. This compromised URE's EMS, part of the ESP at its control center. Further, Enforcement determined that URE did not document nor implement a security patch management program at URE's generating facility.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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, WECC determined that the risk posed by URE's noncompliance was offset by the fact that URE's EMS vendor was performing the assessment and implementation of security patch management for the Cyber Assets at URE's generating station. Furthermore, many of the devices comprising the EMS were relatively new, and therefore few patches were available for assessment during the violation period.

CIP-007-1 R5 (WECC201002549)

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-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 R4 has a "Medium" VRF and a "Severe" VSL.

URE filed a Self-Certification citing noncompliance with CIP-007-1 R5. Specifically, URE stated that it failed to establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, by the date the Standard became mandatory and enforceable for URE.

URE submitted a second Self-Certification citing noncompliance with CIP-007-1 R5. Specifically URE reported that it failed to change passwords for factory default accounts prior to putting any system into service, in violation of R5.2.1. Furthermore, URE reported that it failed to use passwords addressing the requirements of CIP-007-1 R5.2.1 and R5.3. URE stated that the scope of this instance of noncompliance was limited to Cyber Assets associated with the plant control system and Cyber Assets located at URE's generating station.

WECC determined that, consistent with the facts disclosed in URE's Self-Certifications, URE failed to document and implement technical and procedural controls that enforce authentication and accountability for all user activity. WECC also determined that URE failed to document technical and procedural controls that enforce access authentication and accountability pursuant to CIP-007-1 R5. Specifically, WECC determined that URE failed to

ensure passwords were changed annually, as required by R5.3.3. WECC determined that not all passwords included "special" characters, as required by R5.3.2.

WECC determined that URE had a violation of CIP-007-1 R5, R5.2.1, R5.3.2, and R5.3.3 because it failed to document and implement technical and procedural controls that enforce authentication and accountability for all user activity; failed to change passwords for factory default accounts prior to putting any system into service; and failed to ensure passwords were changed annually and included special characters.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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. Specifically, all shared and individual user account activity was monitored and logged. All Cyber Assets and CCAs were located within ESPs and PSPs. The individuals with access to these accounts all completed PRAs and cybersecurity training.[11]

CIP-007-1 R6 (WECC201102592)

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.

[11] WECC determined that the weaknesses of the ESPs and PSP, and the compliance gaps in cybersecurity monitoring identified in this Full Notice of Penalty, did not affect the mitigating factors for this violation.

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 issued a Notice of Self-Certification to URE. URE submitted a Self-Certification citing noncompliance with CIP-007-1 R6 because it failed to ensure that all Cyber Assets within the ESP implement automated tools and organizational process controls to monitor system events related to cybersecurity. Specifically, URE reported that it failed to implement process controls to monitor system events for 60 network devices and 33 servers associated with its control center.

WECC issued a Notice of On-site Compliance Audit to URE. The Audit Team assessed URE's compliance with CIP-007-1 R6, including URE's Self-Certification. Consistent with URE's Self-Certification, the Audit Team determined that URE failed to document organizational processes and mechanisms for monitoring security events, in violation of R6.1. Furthermore, the Audit Team determined that URE failed to implement automated tools or organizational process controls to monitor system events at URE's generating station pursuant to CIP-007-1 R6. The Audit Team forwarded its findings to WECC Enforcement.

WECC Enforcement reviewed the record and determined that URE had a violation of CIP-007-1 R6 because it failed to implement tools and processes to monitor security events for the servers and networking systems associated with its control center, as required by CIP-007-1 R6.1, and failed to implement automated tools or organizational processes at URE's generating station to monitor system events, as required by CIP-007-1 R6.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date 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 did implement tools and processes to

detect cybersecurity events for the majority of CCAs and Cyber Assets within its control center ESP. All Cyber Assets within scope of the violation were contained within ESPs. Access to Cyber Assets within both ESPs was logically and physically controlled and monitored. Furthermore, URE installed tripwires on systems contained within the ESPs, thereby further reducing the risk to the BPS.

CIP-007-1 R8 (WECC201102837)

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 "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of On-site Compliance Audit to URE. URE submitted a Self-Report citing noncompliance with CIP-007-1 R8 for a failure to conduct vulnerability assessments (CVAs) on all Cyber Assets within the ESP. The scope of the Audit included URE's compliance with CIP-007-1 R8, and the Audit Team reviewed URE's Self-Report. The Audit Team reviewed URE's CVA documentation and conducted interviews with URE staff responsible for CVAs. The Audit Team determined that URE failed to conduct a CVA of Cyber Assets comprising URE's EMS and forwarded its findings to Enforcement.

WECC Enforcement reviewed the record and determined that URE had to demonstrate compliance with this Standard as of the date the Standard became mandatory and enforceable

for URE. However, URE deployed a new EMS, a CCA essential to its control center operations. URE initially deferred its CVA for Cyber Assets comprising the EMS until the system vendor completed stability testing. The vendor completed stability testing in the fall. URE, however, failed to conduct a CVA for 118 Cyber Assets and CCAs within its power operations ESP by the end of the year. Because URE completed CVAs for all Cyber Assets and CCAs the spring of the next year, Enforcement determined that the violation period was limited to the six calendar months, as URE did complete its annual assessment for the following year.

WECC Enforcement determined that URE had a violation of CIP-007-1 R8 because it failed to conduct a CVA for 118 Cyber Assets and CCAs within its power operations ESP by the end of the year.

WECC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE through the date URE completed its annual CVA for the next year.

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system BPS. URE did perform a CVA for all Cyber Assets and CCAs outside of its EMS. Furthermore, URE demonstrated that it completed CVAs for the following two years.

CIP-007-1 R9 (WECC201102550)

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 issued a Notice of Self-Certification to URE. URE submitted its Self-Certification citing noncompliance with CIP-007-1 R9. Specifically, URE did not have evidence of annual reviews for CIP-007 documentation at URE's generating station, and it failed to update CIP-007 documentation to reflect modifications to systems or controls within 30 calendar days of completion.

URE submitted a Self-Report that expanded the scope of the noncompliance cited in its Self-Certification. In its Self-Report, URE reported that it did not conduct an annual review of CIP-007 documentation for its power operations EMS.

WECC SMEs reviewed URE's Self-Certification and Self-Report and confirmed that URE failed to provide evidence of an annual review of CIP-007 documentation for Cyber Assets associated with URE's generating station and control center. The SMEs forwarded their findings to Enforcement.

Enforcement reviewed the record and determined that URE was required to reach compliance with CIP-007-1 R9 as of the date the Standard became mandatory and enforceable for URE for Cyber Assets at its control center. URE was required to demonstrate compliance with CIP-007-1 R9 by the end of the following year for URE's generating station. Enforcement determined that URE failed to demonstrate that it annually reviewed and updated CIP-007 documentation for both facilities. Furthermore, Enforcement determined that URE failed to document changes resulting from modifications to the system or controls within 90 calendar days of the change.[12]

WECC determined that URE had a violation of CIP-007-1 R9 because it failed to demonstrate that it annually reviewed and updated CIP-007 documentation for its control center and URE's generating station.

WECC determined the duration of the violation to be from the date the Standard first became mandatory and enforceable for URE through the date 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. Specifically, the risk posed by the violation was offset by the fact that URE provided records for changes made to systems and controls. However, the records were not incorporated into URE's CIP-007 documentation.

CIP-009-1 R5 (WECC201102556)

The purpose statement of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these

[12] CIP-007-1 R9 required entities to revise documentation within 90 calendar days of a modification or change. With the implementation of CIP-007-2 R9 on April 1, 2010 and CIP-007-3 R9 on October 1, 2010, entities were required to update documentation within 30 days of a modification or change to systems or controls.

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 R5 provides: "Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

CIP-009-1 R5 has a "Lower" VRF and a "Severe" VSL.

WECC issued a Notice of Self-Certification to URE. URE submitted its Self-Certification citing noncompliance with CIP-009-1 R5. URE submitted a Self-Report citing noncompliance with CIP-009-1 R5.[13] Specifically, URE self-reported that it failed to perform annual testing of information essential to recovery stored in backup.

WECC SMEs reviewed URE's Self-Report and determined that URE stored backup information in one of three ways: on DVDs; on tapes; or on hard drives. The SMEs reviewed URE's testing information and determined that URE did annually review power operations information stored on tape. The SMEs, however, also determined that URE did not annually test backup information for power operations stored on hard drives and on DVDs. The SMEs determined that URE was in violation of CIP-009-1 R5 and forwarded their findings to Enforcement.

Enforcement reviewed the record and determined that URE was required annually to test power operations backup information as of the date the Standard became mandatory and enforceable for URE. Enforcement determined that URE failed to test backup information stored on hard drives and DVDs for two years.

WECC determined that URE had a violation of CIP-009-1 R5 because it failed to test power operations backup information stored on hard drives and DVDs for two years.

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

[13] WECC determined that the Self-Report would be the appropriate document for the method of discovery as this violation was reported twice.

WECC determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the BPS. URE tested the information stored on tapes but did not test the information on DVDs and hard drives. Furthermore, the scope of the violation was limited to a subset of devices within URE's power operations, and did not include all systems and devices essential to the operation of the control center.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of two hundred ninety-one thousand dollars ($291,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. URE had an internal compliance program (ICP) during the pendency of these violations, which was considered a mitigating factor in the penalty determination.
2. URE's compliance history, which was considered an aggravating factor in the penalty determination;
3. URE self-reported the violations of CIP-003-1 R3, CIP-004-1 R2, CIP-007-1 R9, and CIP-009-1 R6, which WECC considered as a mitigating factor in the penalty determination;[14]
4. URE took voluntary corrective actions to remediate the violations;
5. URE was cooperative throughout the enforcement process;
6. URE completed all applicable compliance directives issued by WECC;
7. There was no evidence of any attempt by URE to conceal the violations;
8. There was no evidence that URE's violations were intentional;
9. The violations did not pose a serious or substantial risk to the reliability of the BPS; and
10. There were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[14] WECC determined that even though URE self-reported the violation of CIP-007-1 R8, self-reporting credit should not be applied because URE failed to identify the noncompliance in its Self-Certification. In addition, WECC prompted URE to review compliance with this Standard by issuing a Notice of On-site Compliance Audit. URE submitted a Self-Certification citing noncompliance with CIP-009-1 R5. URE submitted a Self-Report for a noncompliance with CIP-009-1 R5. Although URE self-reported this violation, because URE submitted its Self-Report 12 days after its Self-Certification, WECC determined that the discovery method should be considered Self-Certification. Therefore, WECC did not apply self-reporting credit for this violation.

After consideration of the above factors, WECC determined that, in this instance, the penalty amount of two hundred ninety-one thousand dollars ($291,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[15]

CIP-002-1 R3 (WECC201102568)
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005373 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify and assess all Cyber Assets located at URE's generating station;
2. Develop a CCA list that identifies all CCAs and is approved by the senior manager;
3. Develop a dedicated compliance program and team to represent enterprise and local URE's generating station level interests in the context of CIP compliance;
4. Develop a comprehensive inventory for all Cyber Assets at URE's generating station, describing CIP-related information for each of the Cyber Assets contained within the inventory, such as operating system version, patch level, and ESP and PSP assignments; and
5. Integrate the comprehensive inventory with the URE's generating station change control and configuration management processes.

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

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

CIP-003-2 R1 (WECC201102569)
URE's Mitigation Plan to address its violation of CIP-003-2 R1 was submitted as complete to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan

[15] *See* 18 C.F.R § 39.7(d)(7).

for this violation is designated as WECCMIT005374 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Make its Policy available in hardcopy form at URE's generating station; and
2. Update internal processes to ensure that a single Policy would be made available at all URE critical facilities.[16]

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

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

CIP-003-1 R3 (WECC201102582)

URE's Mitigation Plan to address its violation of CIP-003-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007398 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review, update, and publish the Policy to align better with the NERC CIP Standards and in consideration of URE's operational environment;
2. Verify that the updated Policy describes the policy exception process;
3. Review exceptions to the Policy to ensure that any existing exceptions are still required and valid, and document any newly identified exceptions;
4. Follow the Policy exception process to document any new exceptions; and
5. Obtain approval from the CIP senior manager (or delegates) for any newly identified exceptions to the Policy.

[16] Although training was not specifically included in the Mitigation Plan, WECC determined that URE's employees were trained and were given a copy of URE's Policy.

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

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

CIP-003-1 R4 (WECC201102581) and CIP-003-1 R5 (WECC201102587)

URE's Mitigation Plan to address its violation of CIP-003-1 R4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007451 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-003-1 R5 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007450 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Review and verify the list of designated personnel who are responsible for authorizing logical or physical access to protected information;
2. Review and update the IPP and any supporting operating procedures;
3. Identify protected CIP information;
4. Classify protected information by following the security classification guidelines described in the IPP;
5. Develop and implement the program for managing access to protected CIP information;
6. Implement the documented IPP, including the program for managing access to protected CIP information;
7. Assess adherence to the IPP, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment; and

8. Assess and document the processes for controlling access privileges to protected information.[17]

URE certified that the above Mitigation Plans requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

WECC will verify that URE's Mitigation Plans were completed.

CIP-004-1 R2 (WECC201102589)

URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted as complete to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007168 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Reassign the task of tracking cybersecurity training of personnel at URE's generating station from plant personnel to the URE's NERC compliance personnel;
2. Review the list of personnel (employees and vendors or contractors) that have CIP access (PSP and electronic access) at URE's generating station, and compare it with training records;
3. Verify with plant management that personnel that have CIP access will continue to need CIP access;
4. Suspend or disable CIP access for personnel who have not taken the annual cybersecurity training. Provide training to those personnel, and reinstate CIP access thereafter;
5. Maintain, on an ongoing basis, the current and complete list of personnel who have CIP access and their most recent annual training dates;
6. Monitor training expiration dates of personnel, and schedule and deliver training prior to annual training expiration dates. If training is not taken by identified dates, access management procedures will be invoked and followed to manage CIP access;

[17] WECC determined that although training was not specifically mentioned in the Mitigation Plan, the Mitigation Plan proposal required implementation of changes included in the Mitigation Plan. WECC ensured that all new policies were communicated to the employees involved.

7. Reassign the task of maintaining, coordinating reviews, and updating the cybersecurity training used at URE's generating station from plant personnel to the URE's NERC compliance personnel;
8. Review all cybersecurity training sets used at URE's generating station and consolidate and update these into one training specific to URE's generating station. In conjunction with the corporate cybersecurity training, this URE's generating station-specific training covers CIP-004-3 R2.2.1 through R2.2.4;
9. Roll out the URE's generating station-specific training (with the corporate cybersecurity training) at URE's generating station;
10. Schedule annual reviews and complete any necessary updates to the cybersecurity training program used at URE's generating station (the URE corporate training and the URE's generating station-specific training); and
11. Provide cybersecurity training to its employees.

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

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

CIP-004-3 R4 (WECC201102591)

URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007523 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify and evaluate mechanisms for physical access and electronic access to CCAs at URE's generating station, as necessary;
2. Develop and update the processes (request, approval, implementation, revocation) for managing authorized cyber or authorized unescorted physical access to CCAs at URE's generating station;
3. Implement the processes and procedures for access management at URE's generating station;

4. Develop and update the procedures for the quarterly CCA access list reviews;
5. Review and update the CCA access list (including the specific access rights) based on the updated and newly developed procedures; and
6. Provide training.

WECC will verify that URE's Mitigation Plan was completed once URE submits its Certification of Completion.

CIP-005-1 R1 (WECC201102574)

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007524 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Document the ESPs at URE's generating station;
2. Establish and configure electronic access controls (EACs);
3. Review and verify EAC processes and documentation to support CIP-005-3 R2.5 (i.e., processes for access request and authorization, the authentication methods, the review process for authorization rights per CIP-004 R4, and the controls used to secure dial-up accessible connections);
4. Develop, document, and implement electronic or manual processes for monitoring and logging access at ESP access points;
5. Establish mechanisms for reviewing CIP-005-3 documentation and ensuring the maintenance of electronic access logs; and
6. Verify, document, and implement protective measures for the EACs and Cyber Assets used in the access control and monitoring of the ESP per CIP-005-3 R1.5.

WECC will verify that URE's Mitigation Plan was completed once URE submits its Certification of Completion.

CIP-006-1 R1 (WECC201102596)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this

violation is designated as WECCMIT007448 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Verify and document that all Cyber Assets inside the ESP, including CCAs and Cyber Assets used in the access control and monitoring of the ESPs, reside within an identified six-wall PSP;
2. Identify and document all physical access points to PSPs, including the measures to control access to those access points;
3. Review and update processes, tools, and procedures to monitor physical access to the PSPs;
4. Verify that the documented visitor control program for visitors (personnel without authorized unescorted access to a PSP) includes, at a minimum, the following:
    1. Use of logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from PSPs; and
    2. Continuous escorted access of visitors within the PSPs;
5. Develop the list of Cyber Assets that authorize and log access to the PSPs, exclusive of hardware at the PSP access point such as electronic lock control mechanisms and badge readers;
6. Review the appropriate use of physical access controls, including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls;
7. Review access management processes on access authorization requests and revocation of access authorization, in accordance with CIP-004-3 R4;
8. Verify, document, and/or implement protective measures for the physical access control systems; and
9. Implement the updated procedures.

WECC will verify that URE's Mitigation Plan was completed once URE submits its Certification of Completion.

CIP-007-1 R1 (WECC201102578)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007449 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify personnel, roles, and responsibilities for creating, implementing (using), and maintaining cybersecurity test procedures in a manner that minimizes adverse effects on the production system or its operation;
2. Review and update process documentation and testing procedures to address CIP security testing requirements;
3. Establish a test environment that reflects the production environment;
4. Create backup images for CIP Cyber Assets and establish mechanisms that allow backups to be retrieved to use for testing and simulations; and
5. Develop testing documentation, and train its employees for testing.

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

WECC will verify that URE's Mitigation Plan was completed after it finishes its review of the Certification of Mitigation Plan Completion documents.

CIP-007-1 R2 (WECC201102579)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007361 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Conduct research and data collection of ports and services in use;
2. Document the functions of each port and service required for normal and emergency operations and the reason why the port or service is open or running;

3. Disable all ports and services except for those required for normal and emergency operations; and
4. Establish a process for ensuring ports and services are managed.

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

WECC will verify that URE's Mitigation Plan was completed after it finishes its review of the Certification of Mitigation Plan Completion documents.

CIP-007-1 R3 (WECC201102580)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007362 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review and verify the CIP Cyber Asset inventory;
2. Establish test procedures and a test bed that can be used for testing security patches prior to release;
3. Establish a mechanism to track security patches for CIP Cyber Assets. For each CIP Cyber Asset, identify the resources for obtaining security patches;
4. Identify the scope of work, personnel, and processes necessary to establish a security patch management program; and
5. Develop and document the security patch management program, including mechanisms for tracking, evaluating, testing, and implementing security patches.

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

WECC will verify that URE's Mitigation Plan was completed after it finishes its review of the Certification of Mitigation Plan Completion documents.

CIP-007-1 R5 (WECC201002549)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007525 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Implement technical and procedural controls for identifying and verifying accounts and their associated access permissions on CIP Cyber Assets;
2. Develop and maintain the list of accounts for CIP Cyber Assets;
3. Implement technical and procedural controls for managing shared accounts on CIP Cyber Assets; and
4. Implement technical and procedural controls for password management and usage on CIP Cyber Assets.

WECC will verify that URE's Mitigation Plan was completed once URE submits its Certification of Completion.

CIP-007-1 R6 (WECC201102592)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007363 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Identify CIP Cyber Assets that generate security event information, and document system configuration methodologies. Identify CIP Cyber Assets where this is not technically feasible, and manage technical feasibility exception (TFE) documentation for those devices;
2. Research and identify the automated tools and process controls to monitor security events on CIP Cyber Assets;
3. Implement automated tools or organizational process controls to monitor security events for CIP Cyber Assets, including mechanisms and controls to detect security monitoring failures. Configure CIP Cyber Assets for security event monitoring, logging,

alerting and system event notifications, and retention of security event logs for at least 90 days. Document and verify configuration;

4. Develop, update, and implement process documentation and procedures to implement and maintain the automated tools and process controls to ensure continuous security status monitoring; and
5. Ensure process documentation and procedures include identifying personnel and resources, roles, and responsibilities.

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

WECC will verify that URE's Mitigation Plan was completed after it finishes its review of the Certification of Mitigation Plan Completion documents.

CIP-007-1 R8 (WECC201102837)

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007398 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review, update, and publish the Policy to align better with the NERC CIP Standards and URE's operational environment;
2. Review exceptions to the Policy to ensure that any existing exceptions are still required and valid, and/or document any newly identified exceptions; and
3. Obtain approval from the CIP senior manager (or delegates) for any newly identified exceptions to the Policy.

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

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

CIP-007-1 R9 (WECC201102550)

URE's Mitigation Plan to address its violation of CIP-007-1 R9 was submitted to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT007399 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Develop and maintain the list of CIP-007 documentation associated with CIP Cyber Assets;
2. Implement a process to manage the annual reviews of CIP-007-3 documentation; and
3. Review and update the change management process to include the review and update of CIP-007-3 documentation when managing changes resulting from modifications to the systems or controls.

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

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

CIP-009-1 R5 (WECC201102556)

URE's Mitigation Plan to address its violation of CIP-009-1 R5 was submitted as complete to WECC. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated as WECCMIT005369 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Incorporate media testing into its NERC CIP-009 backup and recovery drills;
2. Update its procedures to include the media testing procedures; and
3. Enhance its compliance processes to reflect a formal methodology for testing backup media.

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

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[18]
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,[19] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on May 7, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a two hundred ninety-one thousand dollar ($291,000) 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 had an internal compliance program at the time of the violation which WECC considered a mitigating factor, as discussed above;
2. URE's prior violations were considered by WECC;
3. URE self-reported the violations of CIP-003-1 R3, CIP-004-1 R2, CIP-007-1 R9, and CIP-009-1 R6, as discussed above;
4. URE took voluntary corrective actions to remediate the violations;
5. WECC reported that URE was cooperative throughout the compliance enforcement process;
6. URE completed all applicable compliance directives issued by WECC;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

[18] *See* 18 C.F.R. § 39.7(d)(4).
[19] *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).

8. there was no evidence that URE's violations were intentional;
9. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
10. 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 ninety-one thousand dollars ($291,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

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

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

Attachments to be Included as Part of this Notice of Penalty

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

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

b) Public Audit Report, included as Attachment b;

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

i. URE's Self-Certification for CIP-002-1 R3;
ii. URE's Mitigation Plan designated as WECCMIT005373 for CIP-002-1 R3;
iii. URE's Certification of Mitigation Plan Completion for CIP-002-1 R3;
iv. WECC's Verification of Mitigation Plan Completion for CIP-002-1 R3;

d) Record documents for the violation of CIP-003-2 R1, included as Attachment d:

i. URE's Self-Certification for CIP-003-2 R1;
ii. URE's Mitigation Plan designated as WECCMIT005374 for CIP-003-2 R1;
iii. URE's Certification of Mitigation Plan Completion for CIP-003-2 R1;
iv. WECC's Verification of Mitigation Plan Completion for CIP-003-2 R1;

e) Record documents for the violation of CIP-003-1 R3, included as Attachment e:

i. URE's Self-Certification for CIP-003-1 R3;
ii. URE's Mitigation Plan designated as WECCMIT007398 for CIP-003-1 R3;
iii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R3;
iv. WECC's Verification of Mitigation Plan Completion for CIP-003-1 R3;

f) Record documents for the violation of CIP-003-1 R4, included as Attachment f:

i. URE's Self-Certification for CIP-003-1 R4;
ii. URE's Mitigation Plan designated as WECCMIT007451 for CIP-003-1 R4;
iii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R4;

g) Record documents for the violation of CIP-003-1 R5, included as Attachment g:

i. URE's Self-Certification for CIP-003-1 R5;
ii. URE's Mitigation Plan designated as WECCMIT007450 for CIP-003-1 R5;
iii. URE's Certification of Mitigation Plan Completion for CIP-003-1 R5;

h) Record documents for the violation of CIP-004-1 R2, included as Attachment h:

i. URE's Self-Certification for CIP-004-1 R2;
ii. URE's Self-Report for CIP-004-1 R2;
iii. URE's Mitigation Plan designated as WECCMIT007168 for CIP-004-1 R2;

iv. URE's Certification of Mitigation Plan Completion for CIP-004-1 R2;
v. WECC's Verification of Mitigation Plan Completion for CIP-004-1 R2;

i) Record documents for the violation of CIP-004-1 R4, included as Attachment i:

i. URE's Self-Certification for CIP-004-1 R4;
ii. URE's Mitigation Plan designated as WECCMIT007523 for CIP-004-1 R4;

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

i. URE's Self-Certification for CIP-005-1 R1;
ii. URE's Mitigation Plan designated as WECCMIT007524 for CIP-005-1 R1;

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

i. URE's Self-Certification for CIP-006-1 R1;
ii. URE's Mitigation Plan designated as WECCMIT007448 for CIP-006-1 R1;

l) Record documents for the violation of CIP-007-1 R1, included as Attachment l:

i. URE's Self-Certification for CIP-007-1 R1;
ii. URE's Mitigation Plan designated as WECCMIT007449 for CIP-007-1 R1;
iii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R1;

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

i. URE's Self-Certification for CIP-007-1 R2;
ii. URE's Mitigation Plan designated as WECCMIT007361 for CIP-007-1 R2;
iii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R2;

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

i. URE's Self-Certification for CIP-007-1 R3;
ii. URE's Mitigation Plan designated as WECCMIT007362 for CIP-007-1 R3;
iii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R3;

o) Record documents for the violation of CIP-007-1 R5, included as Attachment o:

i. URE's Self-Certification for CIP-007-1 R5;
ii. URE's Self-Certification for CIP-007-1 R5;
iii. URE's Mitigation Plan designated as WECCMIT007525 for CIP-007-1 R5;

p) Record documents for the violation of CIP-007-1 R6, included as Attachment p:

i. URE's Self-Certification for CIP-007-1 R6;
ii. URE's Mitigation Plan designated as WECCMIT007363 for CIP-007-1 R6;

iii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R6;

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

i. URE's Self-Report for CIP-007-1 R8;
ii. URE's Mitigation Plan designated as WECCMIT006757 for CIP-007-1 R8;
iii. URE's Certification of Mitigation Plan Completion for CIP-007-1 R8;
iv. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R8;

r) Record documents for the violation of CIP-007-1 R9, included as Attachment r:

i. URE's Self-Certification for CIP-007-1 R9 ;
ii. URE's Self-Report for CIP-007-1 R9;
iii. URE's Mitigation Plan designated as WECCMIT007399 for CIP-007-1 R9;
iv. URE's Certification of Mitigation Plan Completion for CIP-007-1 R9;
v. WECC's Verification of Mitigation Plan Completion for CIP-007-1 R9;

s) Record documents for the violation of CIP-009-1 R5, included as Attachment s:

i. URE's Self-Report for CIP-009-1 R5;
ii. URE's Mitigation Plan designated as WECCMIT005369 for CIP-009-1 R5;
iii. URE's Certification of Mitigation Plan Completion for CIP-009-1 R5; and
iv. WECC's Verification of Mitigation Plan Completion for CIP-009-1 R5.

A Form of Notice Suitable for Publication[20]

A copy of a notice suitable for publication is included in Attachment t;

[20] *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 charlie.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) 883-6885 (801) 883-6894 – facsimile CWhite@wecc.biz	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director of Enforcement 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Christopher Luras* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz

Sandy Mooy* Senior Legal 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	*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/ Sonia Mendonça

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

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

Sonia C. Mendonça
Assistant General Counsel and Director of Enforcement
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
sonia.mendonca@nerc.net

Edwin G. Kichline
North American Electric Reliability Corporation
Senior Counsel and Associate Director of Enforcement
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council

Attachments