December 29, 2016

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP17-_-000

Dear Ms. Bose:

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

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] with the Commission because Western Electricity Coordinating Council (WECC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from WECC's determination and findings of violations of Critical Infrastructure Protection (CIP) NERC Reliability Standards.

---

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2016). *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) and 18 C.F.R § 39.7(d).

[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.

During the early stages of utilities becoming compliant with NERC Reliability Standards, URE submitted a Self-Certification for 36 CIP violations. At the time, URE stated that the entity's cyber security protections did not comply with NERC Reliability Standards, though cyber security protections were in place using government-issued guidelines.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between WECC and URE. 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 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

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

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002156	CIP-007-1	R1	Medium/ Severe	SC	Moderate	No Penalty
WECC201002157	CIP-007-1	R2	Medium/ Severe			
WECC201002158	CIP-007-1	R3	Lower/ Severe			
WECC201002159	CIP-007-1	R4	Medium/ Severe			
WECC201002160	CIP-007-1	R5	Medium/ Severe			
WECC201002161	CIP-007-1	R6	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002162	CIP-007-1	R7	Lower/ Severe	SC	Moderate	No Penalty
WECC201002163	CIP-007-1	R8	Lower/ Severe			
WECC201002164	CIP-007-1	R9	Lower/ Severe			
WECC201002166	CIP-006-1	R5	Medium/ Severe			
WECC201002169	CIP-006-1	R6	Medium/ Severe			
WECC201002170	CIP-003-1	R4	Medium/ Severe			
WECC201002171	CIP-003-1	R5	Lower/ Severe			
WECC201002172	ClP-003-1	R6	Lower/ Severe			
WECC201002173	CIP-008-1	R1	Lower/ Severe			
WECC201002174	CIP-008-1	R2	Lower/ Severe			
WECC201002176	CIP-004-1	R1	Lower/ Severe			
WECC201002177	CIP-004-1	R2	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002178	CIP-004-1	R3	Medium/ Severe	SC	Moderate	No Penalty
WECC201002179	CIP-004-1	R4	Medium/ Severe			
WECC201002180	CIP-009-1	R1	Medium/ Severe			
WECC201002181	CIP-009-1	R2	Medium/ Severe			
WECC201002182	CIP-009-1	R3	Lower/ Severe			
WECC201002183	CIP-009-1	R4	Lower/ Severe			
WECC201002184	CIP-009-1	R5	Lower/ Severe			
WECC201002186	CIP-005-1	R1	Medium/ Severe			
WECC201002187	CIP-005-1	R2	Medium/ Severe			
WECC201002188	CIP-005-1	R3	Medium/ Severe			
WECC201002189	CIP-005-1	R4	Medium/ Severe			
WECC201002190	CIP-005-1	R5	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
WECC201002198	CIP-003-1	R1	Medium/ Severe	SC	Moderate	No Penalty
WECC201002199	CIP-003-1	R3	Lower/ Severe			
WECC201002200	CIP-006-1	R1	Medium/ Severe			
WECC201002201	CIP-006-1	R2	Medium/ Severe			
WECC201002202	CIP-006-1	R3	Medium/ Severe			
WECC201002203	CIP-006-1	R4	Medium/ Severe			

Common Risk Statement for all Violations

WECC determined that each of these violations posed a moderate and not serious or substantial risk to the reliability of the bulk power system (BPS). Although URE had not implemented all processes to become compliant with CIP standards and requirements, WECC confirmed that URE had implemented cyber security practices, procedures, and technologies different than those prescribed by NERC Reliability Standards CIP-002-009. For this reason, the risk posed by URE's violations was somewhat reduced.

Common Duration for all Violations

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

Common Certification and Verification Information for all Violations

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

WECC201002156 CIP-007-1 R1 - OVERVIEW

WECC determined that URE did not create or implement cyber security test procedures as required by CIP-007-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify test procedures for any assets that are now identified as Critical Cyber Assets (CCAs) pursuant to CIP-002 R3, that may assist in the development of NERC CIP test procedures and identified baseline security configurations;
2. ensure that test procedures to determine changes in baseline security configurations for each CCA and Cyber Asset located within an Electronic Security Perimeter (ESP) have been developed and documented;
3. ensure that the test procedures developed only validate the minimal ports and services necessary for normal and emergency operations remain enabled; and
4. ensure that a formal tracking capability exists to log the execution of test procedures, successful or failed tests, and any necessary test procedure updates or revisions resulting from test execution.

WECC201002157 CIP-007-1 R2- OVERVIEW

WECC determined that URE did not establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled as required by CIP-007-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing baseline configurations for all assets identified as CCAs pursuant to CIP-002 R3, and verify that the minimal ports and services have been determined for each Cyber Asset accordingly. Also, identify any procedures or other resources utilized to determine the minimal ports and services for each Cyber Asset that may assist in compliance with NERC CIP requirements for minimal ports and services;

2. ensure that the minimal ports and services for each CCA and Cyber Asset within the ESP have been established and documented; and
3. develop, document, and promulgate procedures to ensure that the minimal ports and services are enabled for each CCA and Cyber Asset prior to placement into an operational system.

WECC201002158 CIP-007-1 R2 - OVERVIEW

WECC determined that URE did not 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 ESPs as required by CIP-007-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing patch management processes and procedures that have been afforded to any Cyber Asset that is now identified as a CCA pursuant to CIP-002 R3, that may assist in the development of patch management procedures needed to comply with NERC CIP requirements;
2. implement a cyber security patch management procedure for tracking, evaluating, testing, and installing applicable security patches for all Cyber Assets within an ESP;
3. identify and document a monitoring capability that tracks the release of security updates, patches, vulnerabilities, and vendor notifications for all CCAs and Cyber Assets located within an ESP;
4. ensure that an assessment for applicability of a security patch or upgrade is conducted within 30 days of its availability;
5. ensure that all applicable security patches and upgrades are implemented pursuant to requirements and procedures identified in URE's NERC CIP cyber security policy; and
6. document the compensating measures applied to mitigate the risk of exposure for those patches and upgrades not feasible.

WECC201002159 CIP-007-1 R4 - OVERVIEW

WECC determined that URE did not use antivirus software and other malicious software (malware) prevention tools to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all of its Cyber Assets within the ESP as required by CIP-007-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. determine and document the type of existing antivirus and malware prevention tools required for all Cyber Assets now classified as CCAs or other non-critical Cyber Assets located within a defined ESP;
2. implement the antivirus and malware prevention tools as required based on assessment for all CCAs and Cyber Assets within an ESP;
3. document the approved Technical Feasibility Exception (TFE), where antivirus and malware prevention tools cannot be implemented due to technical limitations;
4. document any compensating measures applied to mitigate the risk of exposure, where TFEs are documented; and
5. establish and document the antivirus and malware prevention tool update process and supporting procedures.

WECC201002160 CIP-007-1 R5 - OVERVIEW

WECC determined that URE did not establish and enforce access authentication of and accountability for all user activity to minimize risk of unauthorized system access as required by CIP-007-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and review any documented authorizations for logical access to Cyber Assets that are now identified as CCAs pursuant to CIP-002 R3. This list will be a basis for personnel lists developed to comply with NERC CIP requirements;
2. implement and/or verify all individual and shared accounts, from the list of individuals with approved authorizations for electronic access and associate privileges;
3. develop and document all technical and operational controls that enforce access authorizations and accountability for user activity;
4. develop and implement procedures to ensure that all user and shared accounts are supported by management authorizations and support a valid "need to know";
5. develop and implement procedures to ensure that all user accounts approved by management are consistent with CIP-003 R5.

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

WECC201002161 CIP-007-1 R6 - OVERVIEW

WECC determined that URE did not ensure that all Cyber Assets within the ESP, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security as required by CIP-007-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify existing security status monitoring capabilities being performed for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the compliance with NERC CIP requirements for CIP-006 R6;
2. determine the scope of Cyber Assets that require security status monitoring, pursuant to the ESPs and hosted CCAs and Cyber Assets determined in CIP-005 R1;
3. design, implement, and document a security status monitoring capability for CCAs and Cyber Assets within the ESP;
4. design, implement, and document the technical and operational procedural mechanism for monitoring and identifying security in support of the security status monitoring capability; and
5. design, implement, and document the security status alerting capability related to the technical and/or operational mechanism implemented.

WECC201002162 CIP-007-1 R7 - OVERVIEW

WECC determined that URE did not establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP(s) as identified and documented in Standard CIP-005, as required by CIP-007-1 R7.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. design, implement, and document procedures to ensure that all data storage media is destroyed or erased from CCAs and Cyber Assets as part of a disposal process;
2. design, implement, and document procedures to ensure that data storage media has been erased prior to redeployment of any CCA or Cyber Asset within an ESP; and

3. promulgate the process that ensures the documentation of all CCA and Cyber Asset disposal and redeployment activities.

WECC201002163 CIP-007-1 R8 - OVERVIEW

WECC determined that URE did not perform a cyber vulnerability assessment of all Cyber Assets within the ESP as required by CIP-007-1 R8.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify the type, scope, and test results for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the development of test procedures and addressing of any identified vulnerabilities, or testing for minimal ports and services;
2. develop and promulgate the CIP vulnerability assessment procedures;
3. develop, execute, and document the results of the execution of the procedures for each identified and discovered Cyber Asset; and
4. prepare a mitigation plan addressing the correction of vulnerabilities identified.

WECC201002164 CIP-007-1 R9 - OVERVIEW

WECC determined that URE did not create the documentation required by CIP-007-1; therefore, it could not review and update the documentation as required by CIP-007-1 R9.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing system security, contingency, and recovery plans to identify documentation for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in the compliance with NERC CIP requirements for CIP-007 R9;
2. identify and place documentation artifacts under management control, including guidance documents, process documents, configuration documents, and event documentation; and
3. develop a process to review all documentation, as part of ongoing maintenance processes annually at a minimum or within 30 days of a change required to support CIP-007 requirements.

WECC201002166 CIP-006-1 R5 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to retain physical access logs as required under CIP-006-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the physical access monitoring requirements in CIP-006 R5 and identify the type of monitoring implemented at all access points;
2. ensure that the physical security plans address and include operational and procedural controls to manage physical access 24 hours a day, seven days a week; and
3. implement the procedural control to monitor physical access identified in the physical security plan.

WECC201002169 CIP-006-1 R6 - OVERVIEW

WECC determined that URE did not implement a maintenance and testing program to ensure that all physical security systems function properly as required under CIP-006-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the Logging of Physical Access requirements in CIP-006 R6 and identify the type of logging or recording implemented;
2. ensure that the physical security plans address and include operational and procedural controls to manage physical access logging 24 hours a day, seven days a week; and
3. implement the physical access logging capabilities and methods identified in the physical security plan.

WECC201002170 CIP-003-1 R4 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy, pursuant to CIP-003-1. Instead, for the protection of CCAs, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document or implement a program to identify, classify, and protect information associated with CCAs as required by CIP-003-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. implement and document a process with supporting procedures to identify, classify, and protect CCA information as defined by CIP-003, R4.1;
2. develop a process and related procedures to execute an annual assessment and review to ensure compliance with CIP-003 R4.1 and classification pursuant to R4.2; and
3. develop a process and related procedures as part of an action plan that tracks the remediation of any identified deficiencies resulting from the assessment identified in Step 2 and pursuant to R4.3.

WECC201002171 CIP-003-1 R5- OVERVIEW

WECC determined that URE did not document or implement a program for managing access to protected CCA information as required by CIP-003-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. create, update, and maintain a list of assigned information control personnel and their scope of responsibilities pursuant to CIP-003 R5.1 and R5.1.1;
2. document a process and/or procedure to verify that the list of assigned information control personnel and their scope of responsibilities and associated access privileges are correct, correspond to industry needs, and identify appropriate roles and responsibilities; and
3. document a process and/or procedures to ensure that the verification process is executed on an annual basis and the results are documented accordingly.

WECC201002172 CIP-003-1 R6 - OVERVIEW

WECC determined that URE did not document or establish a process of change control and configuration management for adding, modifying, replacing, or removing CCA hardware or software, and did not implement supporting configuration management activities to identify, control, and document all entity- or vendor-related changes to hardware and software components of CCAs, as required by CIP-003-1 R6.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify existing configuration management plans (CMPs) where CCAs are included as "configuration items" and formally placed under control of the associated CMP;
2. update and revise the CMP, to identify any configuration items that are defined as CCAs pursuant to CIP-002 R3, and any additional CCAs that may not have been included within the existing CMP that should be included based on NERC CIP requirements outlined in CIP-002 R3.1-R3.3, CIP-005 R1, and CIP-006 R1;
3. update and revise the CMP (including any associated processes, procedures, or documentation) so that all CCAs are identified as such and formally communicate the revisions as part of the change control board's review and approval processes; and
4. maintain all documentation related to this Mitigation Plan as evidence of compliance.

WECC201002173 CIP-008-1 R1 - OVERVIEW

WECC determined that URE did not define methods, processes, and procedures for securing CCAs and non-critical Cyber Assets. Specifically, URE failed to develop and maintain a Cyber Security Incident response plan as required by CIP-008-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. expand or amend the current incident response procedures to ensure that they address various supervisory control and data acquisition installation-type incidents and events and developed procedures for reporting to ES-ISAC;
2. review and revise procedures as necessary to be consistent with URE's requirements for CIP-001 sabotage reporting;
3. review and revise procedures as necessary to be consistent with URE's power resources office, facilities instructions, standards, and techniques;
4. promulgate the revised procedures and establish/identify organizational parties who will have responsibility for incident command reporting/communication reporting, incident control, incident investigation, and resumption of normal operations; and
5. establish and implement a reminder solution for a test of the incident response procedures and plan at least once each year.

WECC201002174 CIP-008-1 R2 - OVERVIEW

WECC determined that URE did not define methods, processes, and procedures for securing CCAs and non-critical Cyber Assets. Specifically, URE failed to retain relevant documentation related to Cyber Security Incidents as required by CIP-008-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to establish and implement a central incident reporting repository for three years of records.

WECC201002176 CIP-004-1 R1 - OVERVIEW

WECC determined that URE did not document and implement security and personnel risk assessment (PRA) programs under CIP-004-1. Specifically, URE failed to establish, maintain, and document a security awareness program as required by CIP-004-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing requirements, training and awareness programs, and current record retention capabilities to identify any such processes that possess applicability for the NERC CIP requirements;
2. design and implement a cyber security awareness program for all employees, vendors, and contractors for all qualifying CCAs pursuant to the requirements of CIP-004 R1;
3. create and maintain a document repository to identify, track, and audit employees, vendors, and contractors for cyber awareness completion; and
4. document and implement a procedure to ensure that the cyber awareness reinforcements are delivered on a quarterly basis.

WECC201002177 CIP-004-1 R2 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to establish, maintain, and document an annual cyber security training program, as required by CIP-004-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. implement a NERC CIP cyber security training program for all personnel with any access to CCAs;

2. implement the cyber security training program for all employees, vendors, and contractors for all qualifying Critical Assets and document attendance and completion of the training; and
3. document and implement a procedure to review and verify that the training was conducted on an annual basis.

WECC201002178 CIP-004-1 R3 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to have a documented PRA program and failed to conduct PRAs as required by CIP-004-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review and ensure that all individuals having authorized cyber or authorized unescorted physical access to CCAs possess an equivalent identify verification and seven-year criminal record check pursuant to CIP 004-R3.1;
2. identify and implement changes to contract clauses and conditions of employment as necessary to enable URE to complete elementary ID and criminal check risk assessments for on-boarding entity and contract staff (prior to staff being granted access);
3. establish and implement a procedure to prompt for personal re-reviews no less frequently than every seven years; and
4. document an annual process to review and ensure that the appropriate documentation for all assessments results is maintained pursuant to CIP-004, R3.3.

WECC201002179 CIP-004-1 R4 - OVERVIEW

WECC determined that URE did not document and implement security and PRA programs under CIP-004-1. Specifically, URE failed to maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs as required by CIP-004-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review existing URE policy and procedures to identify existing requirements, current practices, and the current status of all individuals who have been granted logical and physical access to systems that now include those that may be defined as CCAs;

2. establish requirements and delegated authority to grant logical and physical access to ESPs and Physical Security Perimeters (PSPs);
3. prepare lists of individuals who have been granted logical and physical access based on lists of CCAs, ESPs, PSPs; and
4. document a procedure to ensure that all documentation related to CIP-004 R4 is maintained pursuant to CIP-004.

WECC201002180 CIP-009-1 R1 - OVERVIEW
WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to create CCA recovery plans as required by CIP-009-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. expand or amend the current backup and recovery procedures;
2. promulgate the revised procedures and establish/identify organizational parties; and
3. establish and implement a reminder solution for a test of the backup recovery plan at least once each year.

WECC201002181 STANDARD REQ - OVERVIEW
WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to exercise CCA recovery plans as required by CIP-009-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure local procedures are aligned with program guidance;
2. ensure local procedures are implemented and evidence collection has begun for Critical Asset facilities; and
3. evaluate and confirm cyber security recovery plan testing is implemented.

WECC201002182 CIP-009-1 R3 - OVERVIEW
WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices.

Specifically, URE failed to update CCA recovery plans to reflect changes or lessons learned as required by CIP-009-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to ensure that the recovery plans are updated to reflect any changes or lessons learned as a result of exercises or recovery from an actual incident.

WECC201002183 CIP-009-1 R4 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to have recovery plan(s) that included processes and procedures for the backup and storage of information required for the restoration of CCAs as required by CIP-009-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to ensure that the recovery plans include processes and procedures for the backup and storage of information required to successfully restore each CCA.

WECC201002184 CIP-009-1 R5 - OVERVIEW

WECC determined that URE did not ensure that recovery plans were put in place for CCAs and that these plans follow established business continuity and disaster recovery techniques and practices. Specifically, URE failed to test backup media to ensure that information essential to system recovery is available as required by CIP-009-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to test information essential to recovery that is stored on backup media and establish a procedure to test annually thereafter that the information is available.

WECC201002186 CIP-005-1 R1 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to create and maintain a physical security plan as required by CIP-005-1 R1 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review all serial non-routable access into URE ESPs that rely on entity-owned communications systems and identify all valid access points;

2. review all serial non-routable access into URE ESPs that rely on public-switched telephone networks communications and validate that an ESP is defined for any dial-out or dial-up accessible CCAs that utilize non-routable protocols for that single access point at the dial-up device;
3. validate that the endpoints of communication links between discrete ESPs are included as access points with their respective ESPs and define the access points for each link; and
4. validate that all ESP network diagrams, inventories, and vulnerability assessments identify all interconnected systems, all access points into the ESP, and all Cyber Assets deployed for access control and monitoring of the access points.

WECC201002187 CIP-005-1 R2 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement physical access controls pursuant to CIP-005-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. develop a design for the access points associated with the serial non-routable communication links. The design will provide a Cyber Asset as the access point that is external to the CCA that supports the serial communications;
2. validate that all Cyber Assets utilized in the control and monitoring of the serial non-routable ESP access points are protected in accordance with the measures listed in CIP-005 R1.5. If the appropriate controls could not be provided, TFEs were processed;
3. implement the design and adjust the access control procedures to incorporate the changes; and
4. validate that an approved and documented process exists supporting access requests into the ESP.

WECC201002188 CIP-005-1 R3 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement technical and procedural controls for monitoring physical access to PSPs pursuant to CIP-005-1 R3 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. configure, validate, and document that an electronic monitoring capability is implemented for monitoring and logging non-routable access into the ESP and identified any approved TFE that is applicable to CIP-005 R3.2;
2. implement and document the electronic monitoring capabilities for dial-up accessible CCAs that utilized non-routable protocols; and
3. establish and validate the documented procedure that ensures the timely and periodic review and analysis of electronic access alarms for failed communication attempts to the ESP.

WECC201002189 CIP-005-1 R4 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to record sufficient information to identify individuals and access to PSPs uniquely pursuant to CIP-005-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review previous internal control reviews and security tests and evaluations to identify the type, scope, and test results for any assets that are now identified as CCAs pursuant to CIP-002 R3, that may assist in developing test procedures, addressing any identified vulnerabilities, or testing for minimal ports and services;
2. develop and promulgate the CIP vulnerability assessment procedures. The assessment was completed and documented;
3. employ test procedures and document the results of the test procedures for each identified ESP access point;
4. prepare a mitigation plan addressing the correction of vulnerabilities identified;
5. ensure that the vulnerability assessment verifies ports and services permitted through the access control device, as well as ports and services open for management of the device; and
6. ensure the vulnerability assessment includes the discovery of all ESP access points, including verification that each serial access point is configured as documented in the network diagram.

WECC201002190 CIP-005-1 R5 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to retain physical access logs as required under CIP-005-1 R5.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and place the appropriate documentation artifacts from the following document types under management control: guidance documents, process documents, configuration documents, and event documents;
2. validate documentation process to ensure that management control of documentation meets CIP-005 requirements;
3. review asset inventory spreadsheets for accuracy and validate inventory assets associated with each Critical Asset;
4. review all CIP-005-related documents, including procedures and configuration documents and verify their accuracy; and
5. ensure timely update of change management procedures as required by CIP-005.

WECC201002198 CIP-003-1 R1 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy pursuant to CIP-003-1. Instead, for the management of protection for CCAs, URE relied on a federal cyber security policy. Specifically, URE failed to document or implement a cyber security policy as required by CIP-003-1 R1.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. design the approach, structure, and organization for integrating and documenting the NERC CIP cyber security standards as URE policy;
2. determine structure and organization of cyber security policy for NERC CIP compliance pursuant to existing organizational governance;
3. develop general cyber security policy document that will provide authorization for URE to implement the NERC CIP Standards;

4. develop directives, standards, and associated guidance documents that provide URE staff direction to identify Critical Assets and CCAs and achieve compliance; and
5. identify an activity tracking item to provide an annual prompt no less than 30 days in advance of the annual review date for the policy.

WECC201002199 CIP-003-1 R3 - OVERVIEW

WECC determined that URE did not implement management controls, including a cyber security policy pursuant to CIP-003-1. Instead, for the management of protection for CCAs, URE relied on a federal cyber security policy. Specifically, URE failed to document exceptions in instances in which it could not conform to its cyber security policy, as required by CIP-003-1 R3.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify exceptions from the promulgated policy that are necessary for installed and planned cyber systems that qualify under the NERC CIP requirements;
2. review submitted exception request rationale for reasonability and risk and forward qualifying exception requests to the senior manager responsible for final review and signature;
3. secure the approval of the NERC CIP policy exceptions from the senior manager responsible for the NERC CIP effort; and
4. formally document the reviews and approvals.

WECC201002200 CIP-006-1 R1 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a federal cyber security policy. Specifically, URE failed to create and maintain a physical security program as required by CIP-006-1 R1 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. develop the security plan template and promulgate it to all system owners for an initial assessment regarding the scope of impact to existing physical security systems and security operations;
2. perform initial reviews and comments. Revisions to the template or process updates were considered accordingly;

3. submit final physical security plans;
4. establish and implement a reminder solution for an annual review;
5. implement the physical security plans per NERC CIP Requirements CIP-006 R2 through R8; and
6. review physical security plans.

WECC201002201 CIP-006-1 R2 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a federal cyber security policy. Specifically, URE failed to document and implement physical access controls pursuant to CIP-006-1 R2.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. identify and inventory all existing or planned physical security systems that authorize and/or log access to ESPs and CCAs;
2. conduct initial assessments and cost estimations to align the existing physical security systems identified;
3. ensure that all final PSPs submitted as final pursuant to CIP-006 R1, included and addressed compliance with the standards;
4. execute any associated design, procurement, or installation plans; and
5. complete all tasks and activities associated with plans identified.

WECC201002202 CIP-006-1 R3 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to document and implement technical and procedural controls for monitoring physical access to PSPs pursuant to CIP-006-1 R3 and its sub-requirements.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. review to ensure that all prerequisites have been completed;
2. verify that all Cyber Assets used in the access control and/or monitoring of the ESPs reside within a PSP;

3. ensure that Cyber Assets that exist within a PSP are documented in the physical security plan; and
4. develop and execute plans to move or encapsulate the Cyber Assets within a PSP, for Cyber Assets that do not exist in a PSP.

WECC201002203 CIP-006-1 R4 - OVERVIEW

WECC determined that URE did not ensure physical security and implement a physical security program for the protection of CCAs. Instead, URE relied on a cyber security policy conforming to federal guidelines. Specifically, URE failed to record sufficient information to identify individuals and access to PSPs uniquely pursuant to CIP-006-1 R4.

URE submitted its Mitigation Plan to address the referenced violation. URE's Mitigation Plan required URE to:

1. ensure that the physical security plans developed pursuant to CIP-006 R1 address the physical access control requirements in CIP-006 R4 and identify the type of physical access methods implemented at all access points;
2. ensure that the PSPs address and include operational and procedural controls to manage physical access 24 hours a day, seven days a week; and
3. implement all physical access control capabilities and methods identified in the physical security plan.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed no penalty for the referenced violations. In reaching this determination, WECC considered the following factors:

1. the instant violations constitute URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-certified the violations;
3. URE was cooperative throughout the compliance enforcement process;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations posed a moderate and not a serious or substantial risk to the reliability of the BPS; and

6. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, WECC has assessed no penalty for the referenced violations.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on September 29, 2016 and approved 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that no penalty is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

[4] *See* 18 C.F.R. § 39.7(d)(4).

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

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

Jim Robb* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6853 (801) 883-6894 – facsimile jrobb@wecc.biz Ruben Arredondo* Senior Legal Counsel Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7674 (801) 883-6894 – facsimile rarredondo@wecc.biz Heather Laws* Manager of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 819-7642 (801) 883-6894 – facsimile hlaws@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.	Sonia C. Mendonça* Vice President of Enforcement and Deputy General Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Gizelle Wray* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile gizelle.wray@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline

Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline*
Senior Counsel and Associate Director, Enforcement
Gizelle Wray*
Associate Counsel
North American Electric Reliability Corporation
1325 G Street N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 - facsimile
sonia.mendonca@nerc.net
edwin.kichline@nerc.net
gizelle.wray@nerc.net

cc: Unidentified Registered Entity
Western Electricity Coordinating Council