PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 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. NP14-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because 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-004-3 R4, CIP-005-1 R1, CIP-006-1 R1, and CIP-007-1 R1 through R5, R8, and R9. According to the Settlement Agreement, URE agrees and stipulates to the violations, and has agreed to the assessed penalty of one hundred eighty-five thousand dollars ($185,000), 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 WECC2012009779, WECC2011008709, WECC2012009759, WECC2012009746,

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

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

WECC2012009792, WECC2012009793, WECC2012009794, WECC2012009795, WECC2012009796, WECC2012009797, and WECC2012009798 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 October 30, 2013, 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-2232	WECC2012009779	CIP-002-1	R3	High	$185,000
			WECC2011008709	CIP-004-3	R4; R4.2	Lower	
			WECC2012009759	CIP-005-1	R1	Medium	
			WECC2012009746	CIP-006-1	R1; R1.8	Medium	
			WECC2012009792	CIP-007-1	R1	Medium	
			WECC2012009793		R2	Medium	
			WECC2012009794		R3	Lower	
			WECC2012009795		R4	Medium	
			WECC2012009796		R5; R5.2.3	Medium	

Western Electricity Coordinating Council	Unidentified Registered Entity	NOC-2232	WECC2012009797	CIP-007-1	R8;R8.4	Medium	$185,000
			WECC2012009798		R9	Lower	

CIP-002-1 R3

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. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
>
> 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[4] shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control

[4] Within the text of the CIP Reliability Standards, "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.

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

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

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

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

[Footnote added.]

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

During a Compliance Audit (Compliance Audit), WECC determined that URE had a violation of CIP-002-1 R3. URE documented and implemented a Risk Based Assessment Methodology (RBAM) pursuant to CIP-002-1 R2 and identified Critical Assets based on the outcome of the RBAM. However, URE failed to use this Critical Assets list to identify Critical Cyber Assets (CCAs) pursuant to CIP-002-1 R3. Although URE identified the Critical Assets, it assessed only 20 percent of the Critical Assets as CCAs, thereby failing to assess several substations identified as Critical Assets for associated CCAs essential to substation operations.

WECC determined that URE had a violation of CIP-002-1 R3 because URE failed to assess and list CCAs associated with Critical Assets identified pursuant to CIP-002-1 R2.

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

WECC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, URE failed to assess and identify CCAs associated with Critical Asset substations. The substations were identified as Critical Assets because each substation housed a Remedial Action Scheme (RAS). In assessing substations for CCAs, URE did not assess or identify any CCAs essential to the operation of the RAS scheme at these facilities and did

not provide a null list. The risk to the reliability of the BPS was mitigated by the following factors. URE did identify CCAs at a few control centers. The RAS equipment at the substations are serial connections only and were deemed not to be essential to the function of the facilities. Subsequent review by URE confirmed that there were no CCAs at these facilities.

CIP-004-3 R4

The purpose statement of Reliability Standard CIP-004-3 R4 provides: "Standard CIP-004-3 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-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-004-3 R4 provides in pertinent part:

> 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.
>
> ***
>
> 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-004-3 R4.2 has a "Lower" VRF and a "Moderate" VSL.

URE submitted a Self-Report to WECC stating that it was in violation of CIP-004-3 R4. Specifically, URE failed to revoke access to CCAs within seven days for three employees who retired and no longer required such access. For the first individual, access was revoked approximately one year and four months retirement. For the second individual, access was revoked over seven months after retirement. For the third individual, access was revoked over three months after retirement.

WECC determined that URE had a violation of CIP-004-3 R4.2 because URE failed to revoke access within seven calendar days for personnel who no longer required access to CCAs.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE revoked physical access within seven days of each individual's retirement date. Each of the individuals left URE in good standing. In addition, each of the individuals completed training under CIP-004 R2 and completed a personnel risk assessment under CIP-004 R3. Furthermore, electronic access to CCAs is monitored by URE 24 hours a day, seven days a week.

CIP-005-1 R1

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

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> ***
>
> R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009
>
> ***

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

During the Compliance Audit, WECC determined that URE had a violation of CIP-005-1 R1. Specifically, URE failed to afford Electronic Security Perimeter (ESP) Access Control and Monitoring (ACM) devices the protective measures as specified in CIP-007-1 R1 and R4. Therefore, URE was in violation of CIP-005-1 R1.5. Although URE performed operational testing on the devices, URE failed to create and document a test procedure for the devices to ensure the devices do not adversely affect existing cyber security controls, as required by CIP-007-1 R1. URE also failed to use anti-virus software prevention tools on the devices as required by CIP-007-1 R4.

WECC determined that URE had a violation of CIP-005-1 R1.5 because it failed to afford eight ESP ACM devices the protective measures as specified in CIP-007-1 R1 and R4.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The quality assurance (QA) environment used by URE for operational testing of Cyber Assets prior to deployment included many of the cyber security controls used in the production environment. The QA environment is equipped with an antivirus system, user authentication, system event logging, and the use of an open source host-based intrusion detection system (IDS) on system servers. Operational testing of Cyber Assets in the QA environment would have detected some changes to the security measures prior to Cyber Asset deployment in the production environment. The affected devices were secured behind layered security measures. Access through the ESP ACM devices was controlled and monitored. URE implemented a system event monitoring system, which operates 24 hours a day, seven days a week, to alert staff to any cyber security event.

CIP-006-1 R1

The purpose statement of Reliability Standard CIP-006-1 R1 provides in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets."

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> ***
>
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.
> >
> > ***

CIP-006-1 R1.8 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC determined that URE had a violation of CIP-005-1 R1. WECC issued URE a data request for evidence demonstrating that physical security perimeter (PSP) physical access control and monitoring (PACM) devices were afforded protective measures under R1.8, including protections specified in CIP-005 and CIP-007. URE submitted its data request response in which URE outlined protections afforded to CCAs, but did not provide evidence of protective measures afforded to Cyber Assets used in PACM. URE determined that CIP-005 and CIP-007 were not applicable because Cyber Assets provisioning PACM to the PSP are not considered CCAs.

WECC determined that the plain language of CIP-006-1 R1.8 requires that entities afford Cyber Assets provisioning PACM the protections specified in CIP-005-1 R1 and R2, and CIP-007-1 R1, R2, R4, R5, R6, and R8. Therefore, CIP-006-1 R1.8 requires entities to demonstrate that Cyber Assets within the scope of CIP-006-1 R1.8 are protected as described therein.

WECC determined that URE had a violation of CIP-006-1 R1.8 because URE failed to ensure Cyber Assets provisioning PACM were afforded protective measures specified in CIP-005-1 R1 and R2, and CIP-007-1 R1, R2, R4, R5, R6, and R8.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The physical access control system (PACS) is stand-alone and independent of ESPs containing CCAs or Cyber Assets. Therefore, electronic access to PACM devices would not compromise CCAs or Cyber Assets within the ESP. In the event PACM devices were compromised, URE has a backup and recovery process. Physically, the PACM devices are secured behind a layered security perimeter. The PACM devices are located within a locked facility. Physical access to the facility is monitored and controlled, 24 hours a day, seven days a week, by onsite security guards at the main entrance.

CIP-007-1 R1

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

CIP-007-1 R1 provides:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
>
> R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
>
> R1.3. The Responsible Entity shall document test results.

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

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R1.1. Upon review of URE's CIP change control and CIP change request procedures, WECC found that URE change control procedures did not require URE to assess or test changes to existing ESP cyber security controls. Although the testing performed by URE assessed operability of new Cyber Assets deployed within the ESP, WECC determined that the procedures in place did not address cyber security testing and also did not ensure that the addition of new Cyber Assets or changes to the existing ESP would not compromise existing security controls.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE testing procedures addressed Cyber Asset operability, not existing cyber security controls. The risk to the reliability of the BPS was mitigated by the following factors. All changes were tested through URE's Development Environment and QA testing before being deployed within the ESP. Testing conducted as part of the QA process includes, by default, some testing of cyber security controls. In the event that security controls are impacted, URE

ESPs are secured by user authentication, system event logging, and the use of the host-based IDS on system servers.

CIP-007-1 R2

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.

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R2. Specifically, URE failed to provide sufficient evidence demonstrating that URE documented and implemented a process to ensure that only ports and services required for normal and emergency operations were enabled. URE's Cyber Vulnerability Assessments (CVAs) for two consecutive years merely documented open ports and services without making any assessment as to whether the open ports and services are required for normal and emergency operations.

WECC determined that URE had a violation of CIP-007-1 R2 because URE's process failed to ensure that only ports and services required for normal and emergency operations are enabled.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's testing procedures only inventoried all ports and services without defining or specifically identifying ports and services required for normal and emergency operations. The risk to the reliability of the BPS was mitigated by the following factors. All devices with open ports and services were secured within ESPs and PSPs. All access and use of those Cyber Assets was monitored using the logging server and host-based IDS.

CIP-007-1 R3

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
> >
> > R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R3. Specifically, URE failed to implement a process that tracked, evaluated, and tested applicable non-Microsoft cyber security software patches. In addition, URE failed to assess security patches for a specific company within 30 calendar days of availability, in violation of R3.1.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE did establish and implement a security patch management program for all

Microsoft operating system patches. The assessment of the patches was up-to-date. All devices in scope were monitored at all times using a combination of the logging server and host-based IDS. URE's system was configured for automatic notification in the case of a malicious cyber security event. URE provided evidence that it actively tracks vulnerabilities identified by the National Vulnerability Database and assesses whether the identified vulnerabilities can affect its system.

CIP-007-1 R4

CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus software and other malicious software ("malware") prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the Electronic Security Perimeter(s).
>
> > R4.1. The Responsible Entity shall document and implement anti-virus and malware prevention tools. In the case where anti-virus software and malware prevention tools are not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.
> >
> > R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R4. URE failed to use anti-virus software and other malicious software prevention tools on Cyber Assets, including virtual memory system (VMS) servers and networking equipment used to support URE's Supervisory Control and Data Acquisition system located within two ESPs. In addition, where anti-virus software was not technically feasible, URE failed to include the devices within the scope of a Technical Feasibility Exception (TFE) request.

WECC determined that URE had a violation of CIP-007-1 R4 because URE failed to implement anti-virus software on Cyber Assets and did not submit TFEs where technically infeasible.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE installed anti-virus and malware prevention tools on all a certain operating system-based Cyber Assets. Although the affected devices were not equipped with malware prevention, each device was in a "frozen status" such that no changes could be made. Therefore, the risks posed by malicious software being introduced were limited. The devices were located behind restricted firewalls. All access to the ESPs was monitored 24 hours a day, seven days a week by alerting software.

CIP-007-1 R5

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> ***
>
> R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
>
> ***
>
> R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

CIP-007-1 R5.2.3 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R5. WECC issued a data request for shared account audit trail documentation and copies of URE's procedure for managing shared account access in the event of a personnel change. URE responded that it had no

procedures for creating an audit trail of shared account use, and that it did not have a documented procedure addressing shared account access in the event of a personnel change.

WECC determined that URE had a violation of CIP-007-1 R5.2.3 because URE failed to produce documents evidencing an audit trail of shared account use. In addition, URE failed to document a procedure for managing shared account use in the event of a personnel change.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE maintained a list of all shared account users. URE's system was monitored 24 hours a day, seven days a week for system events. URE limited access to shared accounts to individuals granted specific authorized access. Although URE did not document a procedure for managing shared accounts, URE managed access to shared accounts by changing the password to the shared account any time there was a personnel change. All passwords to shared accounts were changed every 365 days, and passwords were at least six characters long.

CIP-007-1 R8

CIP-007-1 R8 provides in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R8.4. 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 R8.4 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R8. WECC requested URE to disclose its CVA documentation generated for two consecutive years. Upon review of the documentation, WECC determined that URE failed to document and execute action plans used to remediate vulnerabilities detected during the CVA process. URE's action plans did not address or remediate all vulnerabilities identified in the CVA. The action plan for the first year itemizes

vulnerabilities and identifies steps URE will take to remediate; however, neither the first year's action plan document nor any other document provided by URE evidences execution of the action plan. Furthermore, WECC found that the second year's CVA was incomplete because it failed to address multiple vulnerabilities regarding ports and services identified by the CVA.

WECC determined that URE had a violation of CIP-007-1 R8.4 because: 1) URE's action plans addressing vulnerabilities identified in the two years did not satisfy R8.4; 2) URE failed to execute its action plan for the first year; and 3) URE's action plan for the second year did not address vulnerabilities identified by the CVA.

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

WECC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's action plans for the two affected years did not identify vulnerabilities. In addition, URE did not track execution of the action plans. The risk to the reliability of the BPS was mitigated by the following factors. Although URE did not assess which ports and services were required for normal or emergency operation, the CVAs run in the two affected years did identify all open ports and services. URE did begin remediation presented by open ports and services not required by normal and emergency operation. Some vulnerabilities were identified in the two affected years.

CIP-007-1 R9

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 "High" VSL.

During the Compliance Audit, WECC determined that URE had a violation of CIP-007-1 R9. WECC issued URE a data request to provide evidence that all CIP-007 documentation was reviewed and approved in one particular year. In response, URE disclosed that CIP-007 documents were initially reviewed in the year before, but an additional set of approvals were not done in the affected year.

WECC determined that URE had a violation of CIP-007-1 R9 because URE failed to review its CIP-007 documentation during the affected year.

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

WECC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE reviewed its CIP-007 documentation in the two years that bookend the affected year. URE did not make any changes to its CIP-007 programs and procedures in the affected year. Therefore, documentation describing these procedures was up-to-date despite URE's failure to review annually.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, WECC has assessed a penalty of one hundred eighty-five thousand dollars ($185,000) for the referenced violations. In reaching this determination, WECC considered the following factors:

1. the violation of CIP-004-3 R4 constituted URE's second occurrence of a violation of the subject NERC Reliability Standards, which WECC considered an aggravating factor;
2. URE was cooperative throughout the compliance enforcement process;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
5. in addition to the monetary sanction, URE agreed to undertake certain additional actions; 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 determined that, in this instance, the penalty amount of one hundred eighty-five thousand dollars ($185,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[5]

CIP-002-1 R3

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to WECC2. The Mitigation Plan was accepted by WECC and approved by NERC. The Mitigation Plan for this violation is designated

[5] *See* 18 C.F.R § 39.7(d)(7).

as WECCMIT007328 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. formally document the null list of CCA for the URE RAS sites. This task will provide documentation for the null case of CCAs for URE RAS sites and thus resolve any potential ambiguity that any CCAs were not evaluated for URE Critical Assets; and
2. update URE procedure to include a step to evaluate all Critical Assets and document null cases for Critical Assets with each annual assessment. This task will update the URE procedure to specifically require the evaluation and documentation of cases where there are no CCAs associated with URE Critical Assets so as to help prevent them from not being addressed in the future.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-004-3 R4

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 WECCMIT007360 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. hire a full-time CIP-004 subject matter expert (SME) to provide a single point of contact for the provisioning and revocation of access and to provide training to URE staff;
2. provide reinforcement of the applicable timelines for revocation of physical and cyber access to all administrative officers; and
3. reinforce processing timelines through on-site training, which included the proper use of applicable URE forms related to CIP compliance including the supervisor checklist for departing employees, for administrative staff in field divisions. The supervisor checklist was updated to include revocation of CIP access to the departing employee, if applicable.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-005-1 R1

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 WECCMIT007337 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update its procedures for firewalls. These tests will be designed to specifically test the cyber security controls aspects of firewall changes;
    a. testing for major changes such as appliance replacement and operating system changes will include: scans of the firewall for ports and services use (to and through the firewall); testing of firewall event monitoring, alarming and logging; system account review and file integrity checking for software validation; and
    b. testing for minor changes such as access control list modifications will include a scan of the firewall for ports and services use through the firewall. These procedures will be added to an overall cyber security controls testing procedure that will be incorporated into the URE CIP change control process. A sign-off sheet will be added to the URE CIP change control process such that the process will be checked with each change and signed off for audit related record keeping purposes;
2. add a step to the URE annual CIP CVA self-assessment to check all change control records since the last CVA and verify that the cyber security controls testing has been satisfactorily completed for each change; and
3. submit a TFE for anti-virus and malware software on Cisco firewalls. By filing a TFE for URE networking device anti-virus and malware prevention software, mitigating measures will be documented to address the lack of available tools, thereby mitigating the alleged violation for CIP requirement CIP-007 R4.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-006-1 R1

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 WECCMIT007336 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform a review of the configuration for the PACM devices. This step will serve the purpose of reviewing the current configuration of the PACM devices to determine what additional configuration changes are necessary to bring the devices into full CIP compliance. This will include basic system configuration and ports and services accounting;
2. update configurations and associated documentation to bring devices up to full CIP compliance level. This step will consist of adding the needed elements and making the required configuration changes necessary to bring the devices up to full CIP compliance level. This will include implementing processes for tracking and updating anti-virus and malware prevention software, operating system patches system account management, audit logging, security event monitoring and access control, and all related documentation;
3. add devices to CIP program self-assessment schedule and change control process. This step will add these devices to the CIP program self-assessment schedule and change control process so that these devices will remain in a CIP-compliant state going forward; and

URE submitted a revised Mitigation Plan which required URE to prepare a spreadsheet/log show the dates that the patches were made available and assessed.

CIP-007-1 R1

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 WECCMIT007329 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a procedure for cyber security controls testing with corresponding check-off list. The testing will include a review of technical aspects of the proposed change to determine which of the below relevant security testing needs to occur as minor changes might not require testing of all items:

a. basic port and services scans to identify open/available services;

b. obtain updates and upgrades from authenticated sources;

c. file integrity checking to identify changes in the size of changed files and application of cryptographic hashes, where supplied by the software vendor;

d. review of appropriate user accounts;

e. validation of CIP-specified security functions (access controls, audit logging, monitoring and alerting functions, and anti-virus and malware prevention updates);

f. malware scans on changed devices;

g. where applicable, review of application source code for custom applications; and

2. add a sign-off sheet to the URE CIP change control process so that the process will be checked with each change and signed off for record keeping purposes.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R2

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 WECCMIT007330 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. finalize ports and services list, which will be signed off by the CIP senior manager. This task will consist of having the URE SMEs and technical staff complete the signoff of the current ports and services lists. Two columns will be added to the ports and services spreadsheet; required for normal operations? (y/n) and required for emergency operations? (y/n). Once the list is complete, it will be sent to the URE CIP senior manager and signed off. Any noted services that can be safely disabled will be disabled; and

2. create a document which describes the process of developing future ports and services lists that will detail:

   a. how ports and services are identified for normal or emergency operations;

b. what the approval process will be; and

c. how the list will be maintained.

This step will result in a procedural control that can assure that repeat violations of requirement CIP-007 R2 will not occur. This procedure will be used a part of the URE CIP change control process so that ports and services are properly documented for audit purposes on-going.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R3

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 WECCMIT007331 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a procedure to review patches and record review of patches for all asset types, including sources and check off list. Use vendor supplied reporting tools where possible;
2. develop, for all systems that are subject to CIP requirements, device-specific procedures for tracking and documenting the assessment of software updates for all CIP-protected devices. This will include which resources and sites will be used for checking postings of software updates and sign-off logs to capture records that software patches were tracked, evaluated, assessed, and applied as appropriate; and
3. move assets out of ESPs. These devices are non-CCAs that happen to reside within URE-defined ESPs and do not serve any critical control system functions. Once the devices are removed from the ESPs, the CIP requirements will no longer be applicable to these devices.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 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 WECCMIT007332 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. submit TFEs for relevant devices for anti-virus and malware prevention tools;
2. add anti-virus and malware prevention to devices for a certain operating system;
3. move assets out of ESP. These devices reside in ESPs but are non-CCAs and serve no critical function in support of URE's Critical Assets. By removing these devices from the ESP, the risk of these devices compromising URE's CCAs is mitigated.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R5

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 WECCMIT007333 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create and implement a standard operating procedure for shared account use, with specific instructions to personnel responsible for assigning shared accounts, including the steps to track shared account usage;
2. review current use of shared accounts. This task is a one-time task to account for current use of shared accounts and eliminate use of shared accounts where not necessary. For each shared account, the following actions will be taken as appropriate:
    a. delete the shared account where not absolutely necessary, or
    b. remove users from shared account access where not necessary. The list of shared account users will be updated and documented as the current, official shared user account list; and

3. implement audit logging of shared account use where not currently implemented. For each device that has shared accounts, system account use audit logging options will be examined and configured to generate the required records needed to report shared account use, if they are not already doing so. Where necessary, scripts will be developed to tie end user account use to system account use and provide the basis to report CIP-compliant shared account usage as required by standard CIP-007 R5. If in any case it is not possible to track shared account use through audit logging mechanisms, a manual log will be instituted to track them.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R8

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 WECCMIT007334 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. close out on the CVA plans for the years relevant to the violation. Document current Action Plan, action items and implement plan with execution status tracking and reporting; and
2. update the CVA process to address process of developing and gaining approval for CVA action plans and execution status tracking. The CVA process will include steps for developing and gaining approval for them. This process will specifically address how the results of the CVA are reviewed to determine which items require actions plans and the process of documenting this analysis so that the action plan will address all the items found during the CVA.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. After reviewing URE's submitted evidence, WECC verified that URE's Mitigation Plan was completed.

CIP-007-1 R9

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 WECCMIT007335 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a separate CIP-007 annual documentation review self-assessment with corresponding checklist and signoff;
2. add a formal internal self-assessment to the CIP self-assessment schedule to review the CIP-007-related documentation and include all of the URE CIP procedures at the same time; and
3. develop a check-off list so that a crosscheck will be in place to ensure that none of the document reviews are missed. Adding this self-assessment to the URE CIP annual self-assessment schedule will help ensure that it is completed on time.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to WECC. 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[6]

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,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including WECC's assessment of a one hundred eighty-five thousand dollars ($185,000) 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:[8]

1. the violations constituted URE's second occurrence of a violation of CIP-004-3 R4;

[6] *See* 18 C.F.R. § 39.7(d)(4).
[7] *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] URE did not receive credit for having a compliance program because URE does not have a compliance program.

2. WECC reported that URE was cooperative throughout the compliance enforcement process;
3. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
4. WECC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
5. in addition to the monetary sanction, URE agreed to undertake certain actions;[9] and
6. WECC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred eighty-five dollars ($185,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[9] In addition to the monetary sanction identified, URE agreed to undertake the following actions:

1. Strengthen compliance training and oversight. Create, document, and implement a compliance training program. The program must include training on compliance with applicable NERC Reliability Standards, violation detection, violation reporting, and violation mitigation;
    a. The training program will include measurable performance targets such as: i) time-based goals for submission of compliance documents to WECC; ii) a defined time-period for prompt submission of Self-Reports following discovery of Possible Violations; and iii) a defined time-period to promptly submit Mitigation Plans following Self-Report filings; and
    b. URE must ensure all employees and contractors receive an appropriate level of effective training;
2. Strengthen policies and procedures related to reporting and mitigation by taking the following actions:
    a. Implement policies and procedures that improve communication and collaboration between URE compliance staff and URE operations personnel;
    b. Establish or improve monthly or bimonthly compliance coordination meetings in which operations, planning, technical and compliance groups are in attendance;
    c. Implement internal processes and procedures to quickly detect and report CIP-related violations; and
    d. Implement internal processes and procedures to ensure mitigation activity is tracked and to ensure URE submits requisite documentation to WECC on time;
3. URE must submit a written update to WECC. The update must describe actions completed to date to satisfy terms outlined above. The update must also describe the actions URE plans to undertake to address outstanding items;
4. URE must submit a written report to WECC. The report must describe how URE implemented the above-described actions. URE must also provide evidence, such as training programs and materials, updated procedures, and policies that were created or modified per the settlement terms. The report must include a summary of the changes made to each procedure as applicable, as well as additional information describing the actions URE took to meet the above-described terms; and
5. URE must submit an internal compliance program (ICP) to WECC using the available ICP assessment documentation.

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

Request for Confidential Treatment

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

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

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

Attachments to be Included as Part of this Notice of Penalty

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

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

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

   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007328;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-004-3 R4, included as Attachment c:

   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as WECCMIT007360;

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

d) Record documents for the violation of CIP-005-1 R1, included as Attachment d:
   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007337;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-006-1 R1, included as Attachment e:
   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007336-1;

f) Record documents for the violation of CIP-007-1 R1, included as Attachment b:
   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007329;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-007-1 R2, included as Attachment b:
   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007330;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-007-1 R3, included as Attachment b:
   1. URE's Discovery Record;
   2. URE's Mitigation Plan designated as WECCMIT007331;
   3. URE's Certification of Mitigation Plan Completion;
   4. WECC's Verification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-007-1 R4, included as Attachment b:

1. URE's Discovery Record;
2. URE's Mitigation Plan designated as WECCMIT007332;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

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

1. URE's Discovery Record;
2. URE's Mitigation Plan designated as WECCMIT007333;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion dated;

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

1. URE's Discovery Record;
2. URE's Mitigation Plan designated as WECCMIT007334;
3. URE's Certification of Mitigation Plan Completion;
4. WECC's Verification of Mitigation Plan Completion;

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

1. URE's Discovery Record;
2. URE's Mitigation Plan designated as WECCMIT007335;
3. URE's Certification of Mitigation Plan Completion; and
4. WECC's Verification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Mark Maher* Chief Executive Officer Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (360) 713-9598 (801) 582-3918 – facsimile Mark@wecc.biz Constance White* Vice President of Compliance Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6885 (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, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Chris Luras* Director of Enforcement Western Electricity Coordinating Council 155 North 400 West, Suite 200 Salt Lake City, UT 84103 (801) 883-6887 (801) 883-6894 – facsimile CLuras@wecc.biz

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

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, Enforcement Processing
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

Attachment