CONFIDENTIAL AND NONPUBLIC 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 (URE), 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 SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] of CIP-006-1 R2; CIP-002-1 R3; CIP-004-1 R2, R3, R4; CIP-005-1 R1, R2, R3, R4; CIP-006-1 R1.8; CIP-006-2 R5; CIP-007-1 R2, R5, R6; CIP-007-3 R1; and CIP-007-3a R1 and R3.. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred and seventy-five thousand dollars ($175,000), 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 SERC201000447,

[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.

SERC201000513, SERC201000564, SERC201000565, SERC201000592, SERC201000593, SERC201000594, SERC201000595, SERC2011008316, SERC2011008511, SERC2011008512, SERC2011008513, SERC2011008516, SERC2012011645, SERC2013013123, SERC2013013146, and SERC2013013146 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement by and between SERC 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 (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
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2242	SERC201000447	CIP-006-1	R2	Medium	$175,000
			SERC201000513	CIP-002-1	R3	High	
			SERC201000564	CIP-004-1	R4	Lower	
			SERC201000565	CIP-007-1	R5	Medium	
			SERC201000592	CIP-007-1	R2	Medium	
			SERC201000593	CIP-005-1	R2	Medium	
			SERC201000594	CIP-007-1	R6	Lower	
			SERC201000595	CIP-006-2	R5	Medium	
			SERC2011008316	CIP-005-1	R1	Medium	
			SERC2011008511	CIP-005-1	R3	Medium	

			SERC2011008512	CIP-005-1	R4	Medium	
			SERC2011008513	CIP-006-1	R1; R1.8	Medium	
			SERC2011008516	CIP-007-3a	R1	Medium	
			SERC2012011645	CIP-007-3a	R3; R3.1	Lower	
			SERC2013013123	CIP-004-1	R2; R2.1	Medium	
			SERC2013013146	CIP-004-1	R3	Medium	

CIP-006-1 R2 (SERC201000447)

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

CIP-006-1 R2 provides:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
>
> R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
>
> R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
>
> R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" Violation Risk Factor (VRF) and a VSL of Severe.

URE submitted a Self-Report stating it failed to document and implement operational and procedural controls to manage physical access at all access points to the Physical Security Perimeters (PSP) at all times.

While performing a physical security self-assessment at a facility, URE found it had failed to implement controls to manage access at four doors to four PSPs (one per PSP). Specifically, URE failed to install compliant special locks on these doors. The next day, URE replaced the non-compliant special locks (key cores) on three of the doors. URE permanently disabled the fourth door because another door to this PSP was properly equipped with the special locks.

About a month later, URE performed an on-site review of a facility and found that an additional 23 doors lacked the appropriate special locks. URE staff performed on-site reviews at two other facilities and determined that all other access points to the PSPs were secured.

SERC determined that URE had a violation of CIP-006-1 R2 for failing to document and implement operational and procedural controls to manage physical access at all access points to the PSPs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE brought the access points (doors) into compliance with the Standard.

SERC 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, failing to secure the PSP adequately could have resulted in unauthorized personnel gaining access. This in turn could have led to Critical Cyber Assets (CCAs) being compromised or being rendered inoperable. In addition, this violation involved approximately 80% of PSPs. However, URE had a documented physical security plan and conducted training for the recognition and reporting of suspicious activity for site personnel.

CIP-002-1 R3 (SERC201000513)

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time 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.

CIP-002-1 R3 has a "High" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that it failed to identify and document 10 CCAs within its Critical Assets. While performing a CIP-002 self-assessment at three facilities, URE discovered that it failed to identify and document 10 CCAs. SERC determined that 2 out of the 10 devices had been protected pursuant to the requirements of CIP-003-1 through CIP-009-1.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a second Self-Report to SERC stating that it failed to identify and document a CCA. URE reported that a staff member identified a dial-up line that was installed and connected to a modem. The line provided a backup communication path to the Critical Asset should the existing serial telecommunication link between the control center and the remote terminal unit fail. URE disconnected the dial-up telecommunication link two days after discovery. Therefore, URE had a dial-up accessible CCA for two days.

SERC learned that without the telecommunication link, URE would not have CCAs at its substations because the devices were connected via a serial protocol; therefore, the device would not be identified on a CCA list or on network diagrams.

SERC determined that URE had a violation of CIP-002-1 R3 for failing to develop a list of CCAs essential to the operation of Critical Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE removed dial-up communications from the device at issue in the second instance of violation.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to identify and protect CCAs properly rendered the Critical Asset and all of the associated CCAs at higher risk of exploitation. Eight out of the ten newly-classified CCAs were not protected in accordance with CIP-003-1 through CIP-009-1. However, physical and electronic access to the CCAs was controlled to allow access only by personnel who had completed personnel risk assessments (PRAs) and cyber security training. In addition, the telecommunications link at issue in the second instance was connected for two days and had limited dial-up connectivity, mitigating the potential risk.

CIP-004-1 R4 (SERC201000564)

The purpose statement of Reliability Standard CIP-004-1 provides in pertinent part: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-1 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.
>
> R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

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

URE submitted a Self-Report to SERC stating that it failed to maintain a complete list of personnel with unescorted physical access to CCAs. URE reported that it discovered a URE employee who was mistakenly granted unescorted physical access to a PSP. URE made this discovery after developing a new report to aid with reviewing the physical access rights. The individual had not received the required cyber security training and did not have a PRA performed. SERC learned that the individual, who was given physical and cyber access, did not use the access privileges during the time they were granted. SERC determined that URE failed to maintain a complete list of personnel with authorized cyber and authorized unescorted physical access to CCAs.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a second Self-Report to SERC. Specifically, URE submitted a Self-Report stating that it had identified an individual whose cyber access was not revoked within seven days as required by R4.2. The individual was a contractor, and the contract came to an end. However, the contractor's access was not removed until approximately three months later. The contractor had received the required cyber security training and PRA. SERC determined that, in this instance, URE failed to revoke access to personnel who no longer required such access within seven days.

SERC determined that URE was in violation of CIP-004 R4 for failing to maintain a complete list of personnel with authorized cyber and authorized unescorted physical access to CCAs and for failing to revoke access for personnel who no longer required such access in a timely manner.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE revoked the access of the contractor.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The employee in the first instance was in good standing with the company and had not used the cyber or physical access during the time it had been granted. The contractor in the second instance had cyber security training, a PRA, and had not used the cyber access since the time the contract ended. The contractor had access to four electronic access control and monitoring (EACM) assets and no CCAs.

CIP-007-1 R5 (SERC201000565)

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 R5 provides:

R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.

R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.

R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain enabled, passwords shall be changed prior to putting any system into service.

R5.2.2. The Responsible Entity shall identify those individuals with access to shared accounts.

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the

account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

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

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

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

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

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

URE submitted a Self-Report stating that it failed to require and use passwords consisting of a combination of alpha, numeric, and "special" characters, as technically feasible. URE reported that it had Cyber Assets deployed within the Electronic Security Perimeter (ESP) that could not technically enforce the "special" character requirement, and that it had not filed a Technical Feasibility Exception (TFE) for those devices. SERC learned that URE filed 17 TFEs for these Cyber Assets. SERC determined that URE failed to implement enhanced passwords, as required.

While SERC was performing its assessment of the Self-Report and determining the scope of the violation, URE submitted three additional Self-Reports citing additional instances of violation.

First, URE submitted a Self-Report to SERC stating that it failed to maintain documentation identifying individuals with access to shared accounts. URE reported that it failed to maintain a list of personnel who had access to shared accounts for CCAs, Cyber Assets, and assets used in the access, control, and monitoring of the ESP and PSP. SERC determined that URE failed to identify those individuals with access to shared accounts.

Second, URE submitted a Self-Report to SERC stating that it failed to implement technical and procedural controls that enforced access authentication of, and accountability for, all user activity. There were four issues in the Self-Report. SERC determined that URE failed to change factory default account passwords prior to putting the system into service on approximately two percent of Cyber Assets. Out of the affected Cyber Assets, 85 percent were CCAs. URE also failed to change the password annually on the affected Cyber Assets. Additionally, URE did not ensure that user accounts were implemented as approved by designated personnel. Specifically, URE granted an individual cyber

access to five devices prior to the individual having received authorization. Lastly, URE failed to remove, disable, or rename 5 factory default accounts prior to system deployment. SERC learned that the passwords for the five default accounts were not changed prior to deployment. SERC determined that URE failed to implement the technical and procedural controls that enforced access authentication of, and accountability for, all user activity.

Third, URE submitted a Self-Report to SERC stating that it failed to change the password on a local administrator account on a Cyber Asset annually, as required. SERC determined that URE failed to change each password at least annually, or more frequently based on risk.

SERC determined that URE was in violation of CIP-007-1 R5 for failing to establish and implement technical and procedural controls that enforced access authentication of, and accountability for, all user activity.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when the administrator password at issue in the last instance was changed.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the combination of: 1) failing to implement enhanced passwords and to change passwords on all Cyber Assets within ESPs; 2) failing to implement procedures to minimize and manage the scope and use of default and shared accounts; and 3) failing to ensure that authorized access permissions were consistent with the concept of "need to know," greatly increased the risk of CCAs being compromised and rendered inoperable. However, electronic access monitoring was enabled, and physical access controls were implemented to protect these devices. In addition, personnel with authorized cyber and/or unescorted physical access to the accounts on the Cyber Assets had PRAs on file and had completed cyber security training.

CIP-007-1 R2 (SERC201000592)

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.

R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

R2.3. In the case where unused ports and services cannot be disabled due to technical limitations, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

URE submitted a Self-Report to SERC stating that it failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled. URE reported that it failed to disable ports and services for 41 devices across four facilities including a control center. The devices involved included workstations, servers, and printers. SERC determined that URE failed to establish and document a process to ensure that only those ports and services required for normal and emergency operations were enabled.

While SERC was performing its assessment of the Self-Report and determining the scope of the violation, two additional instances of violation were found.

SERC sent URE an initial notice of a Compliance Audit. Before the Compliance Audit but after the notice, URE submitted a Self-Report to SERC stating that it failed to disable ports and services not needed for normal or emergency operations on CCAs prior to production use. SERC learned approximately 70 percent of relevant CCAs were involved. SERC determined that URE failed to disable other ports and services on these Cyber Assets prior to production use.

URE submitted an additional Self-Report to SERC, reporting that URE discovered that it failed to enable only those ports and services required for normal and emergency operations for one non-critical Cyber Asset. SERC determined that URE failed to enable only those ports and services required for normal and emergency operations with respect to this device.

SERC determined that URE was in violation of CIP-007-1 R2 for failing to establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE updated its applicable documentation.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to disable ports and services that were not required for normal or emergency operations could have allowed unauthorized individuals or malware to gain unauthorized access to or control over CCAs. However, the affected Cyber Assets resided in an ESP and had limited connectivity to outside networks.

CIP-005-1 R2 (SERC201000593)

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."

CIP-005-1 R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
>
> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
>
> R2.5. The required documentation shall, at least, identify and describe:
>
> R2.5.1. The processes for access request and authorization.
>
> R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

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

URE submitted a Self-Report to SERC stating that it failed to implement and did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs.

SERC learned that URE failed to implement an access control model that denies access by default on three electronic access points, which were routers. URE implemented access control list (ACL) rules, which permitted external host access to all ports and services to specific internal hosts within the ESP; however, it failed to include an explicit-deny ACL for the three routers. In addition, URE failed to enable only the ports and services required for operations and monitoring of Cyber Assets within the ESP. URE did not have documentation detailing the required ports and services for its deployed applications; therefore, it failed to enable only those ports and services required. SERC determined that URE failed to implement and did not document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESPs.

While SERC was performing its assessment of the Self-Report and determining the scope of the violation, SERC discovered an additional instance of violation.

During a Compliance Audit (Compliance Audit), SERC determined that URE failed to implement access rules at its electronic access points that restricted traffic to only the ports and services required for operations and monitoring of the Cyber Assets within the ESP. SERC learned that URE's rule set on these firewalls allowed access into the ESP with the use of the "any port" rule, which meant that all of the ports were enabled between source and destination devices. Only access to ports that were required for operating and for monitoring Cyber Assets should have been enabled. SERC determined that URE failed to enable only those ports and services required for operations and for monitoring of Cyber Assets within the ESPs.

SERC determined that URE was in violation of CIP-005-1 R2 for failing to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the ESP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through the present.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement an access control model to deny access by default and only enable those ports and services that were necessary could have resulted in unauthorized breaches of the ESP. However, the ports and services URE enabled were only open from corporate networks, which were protected by firewalls, virtual local area network constraints, and domain and local account security restrictions. In addition, URE had implemented access control policies that required multiple layers of authentication to gain access to the ESP.

CIP-007-1 R6 (SERC201000594)

CIP-007-1 R6 provides:

R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.

R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP- 008.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-007-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to ensure that all Cyber Assets within the ESP implemented automated tools or organizational process controls to monitor system events that are related to cyber security. Specifically, URE reported that it failed to configure logging devices to provide automated or manual alerts for detected cyber security incidents (CSI). SERC learned that URE configured its devices to send system security logs to a centralized logging and monitoring server, which was not configured properly to alert on detected CSIs. SERC learned that URE had several devices that were (i) not configured to log to the centralized logging server, and (ii) not configured to maintain system security logs for the required 90 days. In addition, logs involving a number of Cyber Assets at one Critical Asset were not being collected and reviewed for a period of approximately five weeks. SERC determined that this failure was due to an issue where the account used to log-in to the Cyber Assets was locked out.

While SERC was performing its assessment of the Self-Report and determining the scope of the violation, URE submitted a second Self-Report identifying an additional instance of violation.

SERC sent URE an initial notice of a Compliance Audit. Prior to the Compliance Audit but after the notice was sent, URE submitted a Self-Report to SERC stating that it failed to implement security status monitoring for all Cyber Assets within the ESPs. The Self-Report described two incidences of violation. The first incidence involved 13 Critical Cyber Assets that were deployed before URE could seek one or more TFEs; these devices were unable to log and monitor. The second incidence involved two Cyber Assets that were not issuing alerts and for which URE was not maintaining logs for the required 90 days. SERC determined that URE failed to implement security status monitoring for 14 Cyber Assets within the ESPs.

SERC determined that URE was in violation of CIP-007-1 R6 for failing to implement monitoring tools to provide for automated alerting for events related to cyber security.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when the devices were configured and URE verified logging to the centralized logging server.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to monitor system events that were related to cyber security for its Cyber Assets within the ESPs could have resulted in a security breach going undetected. An undetected security breach could have rendered CCAs inoperable, resulting in the loss of monitoring and/or control of URE's portion of the BPS. In addition, URE's failure to log system

events related to security events could have impaired its ability to conduct an incident response. However, the affected Cyber Assets resided within an ESP and had limited connectivity to outside networks.

CIP-006-2 R5 (SERC201000595)

The purpose statement of Reliability Standard CIP-006-2 provides: "Standard CIP-006-2 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets."

CIP-006-2 R5 provides:

> R5. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-2. One or more of the following monitoring methods shall be used:
>
> - Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
> - Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

CIP-006-2 R5 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to provide continuous monitoring of physical access at all access points to the PSP at all times.

URE staff received an alarm regarding a possible issue with a piece of equipment located within a PSP. The PSP contained a roll-up door, which under normal conditions would be locked in the closed position and electronically monitored at all times. For safety reasons, URE opened the door during the repairs but failed to implement mitigating measures, resulting in the PSP access point not being continuously monitored. Approximately four days later, URE closed the door. SERC reviewed the physical security drawings, which showed that the unsecured door led to the outside of the facility.

SERC determined that URE had a violation of CIP-006-2 R5 for failing to implement the technical and procedural controls for monitoring physical access at all access points to the PSP at all times.

SERC determined the duration of the violation to be from when URE opened the door to the PSP and failed to implement continuous monitoring, through when URE closed the door and resumed continuous electronic monitoring.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PSP was within an area protected by security guards and security fencing. Access was limited by a gate. In addition, personnel performed hourly rounds of the area and verified that there was no unauthorized access for the duration of the violation.

CIP-005-1 R1 (SERC2011008316)
CIP-005-1 R1 provides:

R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.

R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

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

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

Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

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

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

SERC sent URE an initial notice of a Compliance Audit.

Prior to the Compliance Audit but after the notice was sent, URE submitted a Self-Report stating that it failed to afford Cyber Assets used in the access control and/or monitoring of the ESP all of the protective measures specified in CIP-005-1 R1.5. The Self-Report described multiple instances of violation.

SERC reviewed the Self-Report and determined that URE failed to provide the following protective measures. For a group of information repositories, URE failed to identify the correct personnel responsible for authorizing logical or physical access, as required by CIP-003 R5. For a hard drive, URE failed to create proper documentation of the disposal process in its change management ticketing system, as required by CIP-003 R6.

SERC determined that URE failed to afford all of the protective measures listed in CIP-005 R1.5 to all of URE's EACM devices. Specifically, SERC determined that URE's CIP-007 R1 test procedures for its EACM devices lacked the specific details necessary to ensure that significant changes to existing Cyber Assets would not adversely affect existing cyber security controls. SERC learned that URE failed to assess four PDF reader security patches for three EACM devices as required by CIP-007 R3. For two years, access privileges for all of the EACM devices were not reviewed in accordance with Standard CIP-003 R5 and CIP-004 R4. URE failed to use a "special" character for eight EACM devices, in accordance with the enhanced password requirements of CIP-007 R5.3. SERC learned that the devices could not technically enforce the requirement, but URE had not filed for a TFE. URE also failed to change passwords on an annual basis for system accounts on 11 EACM devices. SERC learned that URE failed to document the results of a Cyber Vulnerability Assessment (CVA), its execution status, and the action plan to remediate or mitigate vulnerabilities identified in the assessment for one year. With regard to CIP-009 R1, SERC learned that the recovery plan was not reviewed in one year for one EACM device and a recovery plan had not been created for a different EACM device.

SERC determined that URE failed to afford Cyber Assets used for access control or monitoring of the ESPs the protective measures specified in CIP-005 R1.5.

While SERC was performing its assessment of the above Self-Report and determining the scope of the violation, URE submitted two additional Self-Reports describing additional instances of violation.

First, URE submitted a Self-Report to SERC stating that it failed to identify two non-critical Cyber Assets within a defined ESP. The non-critical Cyber Assets were discovered while performing an on-site review. SERC learned that the devices were located within a location that was not generally accessible during normal business operations. SERC determined that URE failed to identify two non-critical Cyber Assets within a defined ESP.

Second, URE submitted a Self-Report stating that it identified an EACM device that it failed to protect in accordance with CIP-005-1 R1.5. URE found that it had failed to identify a network device as an electronic access point performing access control functions. SERC reviewed the network diagram and verified that URE failed to identify the device as an EACM device and afford it the protective measures of CIP-005 R1.5. SERC determined that URE was in violation of CIP-005-1 R1 because URE failed to identify and document the ESP and all access points to the perimeter.

SERC determined that URE was in violation of CIP-005-1 R1 for failing to identify all access points to the ESPs, as required.

SERC 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.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify and to protect EACM devices could have allowed for the introduction of vulnerabilities to the ESP and the CCAs located therein. However, the Cyber Assets were monitored at all times by personnel. The two non-critical Cyber Assets had a proprietary operating system and no ability to access other networks.

CIP-005-1 R3.2 (SERC2011008511)
CIP-005-1 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.

R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-1 R3.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to implement security monitoring processes to detect and alert for actual unauthorized access into the ESP. SERC learned that while URE's logging and monitoring policy addressed the requirement to detect and alert attempts at or actual unauthorized access, URE failed to implement the policy on four electronic access points. SERC learned that the electronic access points were routers, which had the ability to perform the logging but were not configured to do so.

SERC determined that URE was in violation of CIP-005-1 R3.2 for failing to implement monitoring processes to detect and alert for unauthorized attempts or actual unauthorized accesses.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE updated the devices at issue to log all traffic.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to monitor access to the ESPs could have resulted in unauthorized access going undetected. However, URE's firewalls were configured to log denied traffic, which provided the ability to alert on unsuccessful attempts at unauthorized access.

CIP-005-1 R4 (SERC2011008512)
CIP-005-1 R4 provides:

R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.1. A document identifying the vulnerability assessment process;

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

R4.3. The discovery of all access points to the Electronic Security Perimeter;

R4.4. A review of controls for default accounts, passwords, and network management community strings; and,

R4.5. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

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

During the Compliance Audit, SERC discovered that URE failed to verify that only ports and services required for operations through the access points were enabled. Specifically, SERC learned that URE failed to review ports and services at five access points during URE's annual CVAs.

SERC determined that URE had a violation of CIP-005-1 R4 for failing to include in its annual CVAs a review that verified that only ports and services required for operations were enabled at five access points.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE verified the ports and services on the access points were required for operations.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not performing reviews of its ports and services at electronic access points at least annually, URE may not have been able to identify mis-configurations or overly-broad or legacy access rules, which could have allowed unauthorized access into the ESP. However, URE had deployed an intrusion detection system (IDS) to detect malicious traffic and alert appropriate personnel upon discovery.

CIP-006-1 R1.8 SERC2011008513)
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, SERC discovered that URE failed to afford protective measures for Cyber Assets used in the access control and monitoring of the PSP all of the protections of CIP-006-1 R1.8. SERC learned that URE deployed approximately 70 devices (including microprocessor devices and servers) used in physical access control and monitoring without securing them as required by CIP-006-1 R1.8. Specifically, SERC determined that URE failed to afford the protective measures of CIP-005 R2 and R3 and CIP-007 R2 and R6.

While SERC was performing its assessment of the above Compliance Audit finding and determining the scope of the violation, URE self-reported an additional issue.

URE submitted a Self-Report to SERC stating that it failed to change factory default account passwords on approximately 100 Cyber Assets used in the access control and monitoring of the PSPs prior to putting the devices into service. While URE had a policy that required factory default passwords to be changed prior to the systems being placed into service, it was not followed in this case. SERC determined that URE failed to change factory default account passwords for Cyber Assets prior to putting the system into service, as required by CIP-007 R5.2.

SERC determined that URE had a violation of CIP-006-1 R1.8 for failing to afford Cyber Assets used in the access control and monitoring of the PSP all of the protective measures set forth in the Standard, specifically the protective measures specified in CIP-005 R2 and R3 and CIP-007 R2, R5.2, and R6.

SERC 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.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE's failure to provide adequate protections to its physical access control and monitoring Cyber Assets could have allowed unauthorized access to the assets, resulting in

CCAs being compromised or rendered inoperable. However, URE had an IDS that would identify and alert upon detecting malicious communications traffic, thereby limiting the risk of malicious traffic reaching the devices.

CIP-007-3a R1 (SERC2011008516)

The purpose statement of Reliability Standard CIP-007-3a provides: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s)."

CIP-007-3a 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-007-3, 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-007-3a R1 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to test existing cyber security controls following a significant change to Cyber Assets within the ESP. SERC learned that the significant change occurred when URE executed a script to disable a service running on approximately 70-80 Cyber Assets. URE did not fully execute the test plan once the significant change was complete, and URE failed to document the completed test results to ensure that existing cyber security controls were not affected. SERC determined that URE failed to document the test results, as required.

While SERC was performing its assessment and determining the scope of the violation, URE self-reported an additional issue.

URE submitted a Self-Report to SERC stating that it failed to follow its documented cyber security test procedures when it added a network switch to an ESP. SERC learned that URE failed to perform the required cyber security testing to ensure that the switch did not affect existing cyber security controls within the ESP. SERC determined that URE failed to ensure that a new Cyber Asset did not adversely affect existing cyber security controls.

SERC determined that URE had a violation of CIP-007-3 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls.

SERC determined the duration of the violation to be from when URE completed the significant change to Cyber Assets within the ESP as described in the first instance, through when URE removed the switch referenced in the second incidence from the ESP.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to test significant changes to existing Cyber Assets and to test new Cyber Assets prior to their deployment could have introduced vulnerabilities or modified existing cyber security controls. This in turn could have permitted unauthorized access to CCAs. However, the significant change in the first instance was a script to disable a service, which was unlikely to introduce any new vulnerabilities. The second instance involved a single network switch which resided for five months behind firewalls that provided protection from unauthorized traffic.

CIP-007-3a R3.1 (SERC2012011645)

CIP-007-3a R3 provides:

> R3. Security Patch Management —The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement 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.

CIP-007-3a R3.1 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to document the assessment of security patches for applicability within 30 days of availability. SERC learned that a URE vendor delivered a monthly patch bundle, which included all of the vendor-tested and approved patches. URE received a patch bundle for one month; however, it failed to assess the patches for applicability to the URE environment within 30 calendar days. SERC learned that the patches were for antivirus and operating system security and were applicable to approximately 60 total devices. The patch bundle included 14 patches. Five patches were deemed critical, with the remaining nine being important updates.

SERC determined that URE had a violation of CIP-007-3a R3.1 for failing to assess a monthly patch release within 30 days of availability, as required.

SERC determined the duration of the violation to be from 30 days after the patches were made available through when URE completed its assessment of the patches.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The affected Cyber Assets resided in an ESP and had limited connectivity to outside networks. In addition, URE had IDS deployed to monitor network traffic for malicious activity and to alert appropriate personnel of anomalous or suspicious activity.

CIP-004-1 R2.1 (SERC2013013123)

The purpose statement of Reliability Standard CIP-004-1 provides: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-1 R2 provides in pertinent part:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

***

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

URE submitted a Self-Report to SERC stating that it granted cyber access to CCAs to personnel who had not completed the required cyber security training.

URE discovered that four employees, who had been granted authorized cyber access, had not completed the required training within 90 days of receiving such authorization. SERC learned that URE had two CIP-required training modules. Module one was for individuals needing only authorized unescorted physical access, and module two was for individuals needing authorized cyber and authorized unescorted physical access. Three of the employees completed module one instead of completing module two; the fourth employee did not complete either module.

SERC determined that URE had a violation of CIP-004-1 R2.1 for failing to ensure that four personnel with authorized cyber access to CCAs were trained within 90 calendar days of such authorization.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when cyber access was revoked.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All of the employees were long-term and in good standing with the company. In addition, three of the employees had completed the required PRAs.

CIP-004-1 R3 (SERC2013013146)
CIP-004-1 R3 provides:

R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3 has a "Medium" VRF and a "High" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-004-1 R3 because it failed to complete the required PRA for one individual within 30 days of granting access to CCAs.

URE identified an employee who had been granted cyber access to an ESP but had not completed the required PRA. SERC staff learned that the employee had been granted access to CCAs prior to the compliance date, and access was immediately revoked upon discovery. The individual gained access through a shared account; therefore it was not possible to determine if the individual accessed the CCAs during the violation period.

SERC determined that URE was in violation of CIP-004-1 R3 for failing to conduct a PRA within 30 days of personnel being granted access to CCAs.

SERC determined the duration of the violation to be from 30 days after the mandatory and enforceable date of the Standard for URE and the date by which the employee's PRA should have been completed, through when URE revoked the employee's access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The employee was given access prior to the mandatory compliance date, was a long-term employee, and was in good standing with the company.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred and seventy-five thousand dollars ($175,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE had prior violations of CIP-004-1 R4 and CIP-005-1 R1, which SERC determined did not warrant an aggravation of the monetary penalty;
2. URE self-reported several of the violations, as discussed above;[4]
3. URE was cooperative throughout the compliance enforcement process;
4. URE had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE agreed to complete several above-and-beyond mitigating actions, as described below; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

In addition to the monetary penalty of one hundred and seventy-five thousand dollars ($175,000), URE agreed to complete several above-and-beyond mitigating actions:

1. URE completed an analysis correlating the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[5] domains with the CIP Standards in order to assess how increasing the maturity indicator level within specific domains may positively impact compliance with the CIP Standards. URE also performed an ES-C2M2 evaluation

[4] SERC did not award self-reporting credit when the Self-Reports were submitted after the issuance of the notice of Compliance Audit.

[5] ES-C2M2 is a capability maturity model developed through collaboration among the White House, Department of Energy, Department of Homeland Security, and representatives of asset owners and operators within the electricity subsector, utilizing the NERC CIP Reliability Standards as a reference. ES-C2M2 is organized into 10 domains and four maturity indicator levels, and each domain is a logical grouping of cyber security practices. The domains' practices are organized by maturity indicator level to define the progression of capability maturity for the domain. ES-C2M2 and its correlation with the CIP Standards can assist URE with the effort to utilize internal controls to maintain compliance with the CIP Standards and ensure reliability of the BPS.

("Evaluation"). The Evaluation consisted of URE's analysis of its maturity indicator levels across the ten domains of ES-C2M2. URE agreed to provide the final Evaluation report to SERC;

2. URE agreed to create and implement an action plan based on the portions of the final Evaluation report associated with the areas that pertain to the CIP Standards. The goal of the action plans will be to enhance the reliability of the BPS and increase URE's maturity indicator level in domains related to the CIP Standards; and
3. URE agrees to provide SERC with quarterly updates regarding the progress of its action plans and to provide SERC with notification and evidence that it completed such action plans, consistent with Section 6.6 of the NERC CMEP.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred and seventy-five thousand dollars ($175,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-006-1 R2 (SERC201000447)
URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install special locks in three doors and permanently disable the non-compliant special lock in one door;
2. perform a walk-down (*i.e.*, on-site review) and disable the additional non-compliant special locks that were identified;
3. perform walk-downs at other URE facilities identified as having CCAs; and
4. develop a checklist and a process for a physical security compliance review, which includes work performed by contractors.

URE certified that the above Mitigation Plan requirements were completed. SERC is reviewing URE's submitted evidence to verify that URE's Mitigation Plan was completed.

[6] *See* 18 C.F.R § 39.7(d)(7).

CIP-002-1 R3 (SERC201000513)

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the CCA list;
2. afford the protective measures of CIP-003 through CIP-009 to the eight CCAs;
3. train applicable personnel on the identification of Cyber Assets and CCAs;
4. complete an IT awareness communication that included reinforcing the usage of a project planning checklist, a project management template update, and a reminder on annual training;
5. evaluate the training needs for applicable staff and complete training addressing such needs;
6. test and publish a policy for validating the disconnected status of a Critical Asset.

CIP-004-1 R4 (SERC201000564)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove access rights of the individual involved in the first instance;
2. verify that all other personnel granted physical access to restricted areas in the facilities with CCAs had completed cyber security training and PRAs;
3. update the database table that feeds queries on training and PRA information to include all accounts, both active and inactive, in order to include terminations, leave of absence, and short- and long-term disability;
4. review all active accounts in the database table.

CIP-007-1 R5 (SERC201000565)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. file the necessary TFE;
2. create master lists for shared accounts used in access and monitoring of the PSP and the ESP, as well as for Cyber Assets within the ESP;
3. update applicable procedures;
4. develop training to address the management of shared accounts and add the training to the training matrix;
5. change passwords on the identified devices and document the change;
6. complete a cyber access request form for the identified employee;
7. disable the identified factory default user accounts;
8. change the password for the local administrator account;
9. perform an extent of condition review at the site in order to identify all of the accounts that fall under the CIP requirements;
10. update the site's shared accounts list with password changes, including the local administration accounts; and
11. review all of the Self-Reports and mitigating actions with other CIP sites for lessons learned.

CIP-007-1 R2 (SERC201000592)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. amend its cyber security policy to call for a TFE to be requested during the installation process of new hardware and software and the "burn-in" period;
2. update its ports and services procedure to request a TFE during migrations, system upgrades, and replacements;

3. review and update change management procedures as necessary;
4. submit necessary TFEs;
5. perform the required ports and services scan and disable ports and services that were not required;
6. remove a non-critical Cyber Asset involved in the last incidence from the network, the CCA list, and the facility's interconnect drawing; and
7. review all of the Self-Reports and mitigating actions with other CIP sites for lessons learned.

CIP-005-1 R2 (SERC201000593)

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. modify access control lists (ACLs) to bring firewalls into compliance;
2. update ACLs to provide comments that better explain the firewall rules;
3. develop network architecture diagram to meet CIP requirements;
4. develop initial action plan for new network device installation;
5. provide an updated action plan for new network device installation;
6. develop an implementation project plan;
7. complete installation of new devices at the applicable sites;
8. provide update on firewall policy changes to applicable personnel;
9. install two-factor authentication as needed on EACM devices;
10. update the firewall policy regarding the protective measures required by CIP-005 R2.2;
11. establish a new naming standard for one set of applicable assets and update the firewall rules;
12. incorporate initial findings for the first set of applicable assets into the new trust rule and update the firewall rules;
13. monitor, then incorporate, any new findings for the first set of applicable assets into the new trust rule;

14. establish a new group naming standard for a second set of applicable assets and update the firewall rules;
15. incorporate the initial findings for the second set of applicable assets into the new trust rule; and
16. monitor, then incorporate, any new findings for the second set of applicable assets into the new trust rule.

In addition, URE will monitor for any new findings for the second set of applicable assets and remove the old trust rule.

The Mitigation Plan is scheduled for future completion.

CIP-007-1 R6 (SERC201000594)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. submit the necessary TFEs;
2. make the technical and procedural changes to the security status monitoring procedure, including automated rules and alerts;
3. integrate correct logging configurations for the devices at issue, where applicable;
4. configure network and firewall to allow logging traffic; and
5. verify successful logging for the applicable devices.

CIP-006-2 R5 (SERC201000595)

URE's Mitigation Plan to address its violation of CIP-006-2 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a review of the CIP requirements regarding restricted access areas for URE facility supervisors; and

2. review the CIP requirements applicable to restricted areas with applicable personnel.

URE certified that the above Mitigation Plan requirements were completed. SERC is reviewing URE's submitted evidence to verify that URE's Mitigation Plan was completed.

CIP-005-1 R1 (SERC2011008316)

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. verify and document the ports and services in operation for the missed devices;
2. document and implement the appropriate use banner for the missed devices;
3. create the required recovery plans for the missed devices;
4. modify the backup and restore procedures;
5. complete review of the Active Directory (AD) owners of all of the information repositories where applicable;
6. change AD ownership to the designated information repository owners;
7. create procedures to note that the repository list and the AD approvers will be updated by the analyst performing the change in the repository owner where the AD group permissions are leveraged;
8. amend the CCA information repository list description to include direction that changes to the list should also be reflected in procedures and documentation;
9. review the Cyber Asset disposal and redeployment process with the team responsible for completing the disposals and redeployments;
10. document future disposal/redeployment in the ticketing system;
11. initiate network isolation project;
12. conduct a project status update;
13. develop new roles and responsibilities for network support;
14. install application clients as needed on EACM devices;

15. update the firewall policy regarding the protective measures required by CIP 005 R2.2;
16. enable two-factor authentication for interactive access into the demilitarized zone;
17. update the testing procedure to include specific details requiring the use of the change control, configuration management, and cyber security testing procedure;
18. assess and apply current security patches;
19. remove software from the servers;
20. add identified user accounts to the master account list;
21. conduct the annual review of access privileges for identified user accounts;
22. amend a TFE;
23. change the group policy for devices integrated with the AD to require a password change every 90 days;
24. change the passwords on the applicable systems;
25. submit a TFE;
26. implement the use of change tickets to document the execution status in the mitigation plans;
27. update the applicable procedure with instructions on how to fill out a mitigation plan to include the step of providing change ticket information;
28. complete the disaster recovery (DR) annual review for EACM 1;
29. develop a DR procedure for EACM 2;
30. revamp DR drills to require annual reviews in advance of drill;
31. review the event with applicable personnel and go over lessons learned;
32. create and submit TFE(s) for the requirements the applicable device cannot meet;
33. obtain a quote for field service support to convert devices to achieve compliance with the Standard;
34. consult vendor regarding the impact of scanning the device which performs a critical function; and
35. change out devices and update site CCA/non-CCA list.

CIP-005-1 R3 (SERC2011008511)

URE's Mitigation Plan to address its violation of CIP-005-1 R3 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the electronic access points to include logging of all accepted traffic;
2. develop an action plan for the installation of new network devices;
3. install the new network devices; and
4. update the policy on the new devices to log all traffic including accepts, drops, and denies.

CIP-005-1 R4 (SERC2011008512)

URE's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update its network architecture diagram;
2. complete annual review firewall rule sets and recommend rules for modification or removal for each identified site to ensure that only ports and services required for operations at all access points were enabled;
3. update procedure document to require a review of the firewall policy as part of the annual CVA;
4. install new network devices and develop data flows, to be used in developing baselines for the ports and services component of the CVA; and
5. review and finalize the data flow diagram to demonstrate the required ports and services on specific nodes.

CIP-006-1 R1.8 SERC2011008513)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation

Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. afford the missed protective measure(s) to the involved Cyber Assets;
2. create an add/remove checklist for cyber assets used in the access control and monitoring of the PSP and the ESP to account for change and configuration management issues and link to the applicable procedures;
3. provide training on the checklist;
4. change the factory default passwords on the involved Cyber Assets;
5. revise the applicable procedure to clarify responsibility for password maintenance on physical access control devices and to include a checklist for the addition, replacement, and retirement of assets; and
6. train the applicable personnel on the password administration requirement of URE's cyber security policy.

CIP-007-3a R1 (SERC2011008516)

URE's Mitigation Plan to address its violation of CIP-007-3a R1 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update its applicable security test;
2. update its applicable procedure;
3. review the updated documents with CIP subject matter experts;
4. implement software to capture user account activities and ports and services before and after significant changes; and
5. publish the updated documents.

URE certified that the above Mitigation Plan requirements were completed. SERC is reviewing URE's submitted evidence to verify that URE's Mitigation Plan was completed.

CIP-007-3a R3.1 (SERC2012011645)

URE's Mitigation Plan to address its violation of CIP-007-3a R3.1 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. assess and install the security patches for the missed month;
2. verify that all patches sent contained previous releases;
3. verify that the previous month's patches were installed; and
4. move responsibility for patch assessment to a different group.

CIP-004-1 R2.1 (SERC2013013123)

URE's Mitigation Plan to address its violation of CIP-004-1 R2.1 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke cyber access for the involved employees;
2. consolidate the two training modules into one module;
3. create a CIP training program procedure for the business group involved; and
4. add the required CIP-004 R2 training to the business group's annual CIP training matrix.

CIP-004-1 R3 (SERC2013013146)

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke access for the involved employee; and

2. create a training program procedure for the business group involved that requires a PRA prior to granting individuals unescorted access to CCAs.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[7]

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,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 23, 2013. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a one hundred and seventy-five thousand dollar ($175,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

In reaching this determination, the NERC BOTCC considered the following factors:

1. URE had prior violations of CIP-004-1 R4 and CIP-005-1 R1, which SERC determined did not warrant aggravation of the monetary penalty, as discussed above ;
2. URE self-reported several of the violations, as discussed above;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;

[7] *See* 18 C.F.R. § 39.7(d)(4).

[8] *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).

7. URE agreed to complete several above-and-beyond mitigating actions, as described above; and
8. 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 and seventy-five thousand dollars ($175,000), in addition to URE's above-and-beyond mitigating actions relating to its analysis and evaluation of the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), 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.

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

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

John R. Twitchell*
VP and Chief Program Officer
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8205
(704) 357-7914 – facsimile
jtwitchell@serc1.org

Andrea B. Koch*
Director, Enforcement
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704)940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

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

Marisa A. Sifontes*
General Counsel
Maggie A. Sallah*
Senior Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7775
(704) 357-7914 – facsimile
msifontes@serc1.org
msallah@serc1.org

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

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: SERC Reliability Corporation