PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 31, 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# NCR 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-002-1 R1, CIP-002-1 R2, CIP-004-1 R4, CIP-005-3a R1, CIP-005-1 R2, CIP-005-1 R3, CIP-005-3a R5, CIP-006-1 R1.1, CIP-006-1 R1, CIP-006-3c R5, CIP-006-3c R5, [4] CIP-006-3c R6, CIP-007-1 R1, CIP-007-1 R2, CIP-007-3a R4, CIP-007-1 R5, CIP-007-1 R6, CIP-007-3 R7, and CIP-007-3a R7. According to the Settlement Agreement, URE admits to the violations and has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to

[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.

[4] URE has two violations of CIP-006-1 R1 (NERC IDs: SERC2013012006 and SERC2011008003) and two violations of CIP-006-3c R5 (NERC IDs: SERC2012011337and SERC2013011700) included in this Full Notice of Penalty.

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 SERC2011007982, SERC2011007983, SERC201000505, SERC2012011336, SERC2013012272, SERC201000622, SERC2012010981, SERC2013012006, SERC2011008003, SERC2012011337, SERC2013011700, SERC2011007999, SERC201000623, SERC2011007873, SERC2012010000, SERC2012009999, SERC201000621, SERC2011008271, and SERC2013012005 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 December 20, 2013, by and between SERC 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
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2237	SERC2011007982	CIP-002-1	R1	Lower	$250,000
			SERC2011007983	CIP-002-1	R2	High	
			SERC201000505	CIP-004-1	R4	Lower	
			SERC2012011336	CIP-005-3a	R1	Medium	
			SERC2013012272	CIP-005-1	R2	Medium	
			SERC201000622	CIP-005-1	R3	Medium	
			SERC2012010981	CIP-005-3a	R5	Lower	
			SERC2013012006	CIP-006-1	R1; R1.1	Medium	

			SERC2011008003	CIP-006-1	R1	Medium	
			SERC2012011337	CIP-006-3c	R5	Medium	
			SERC2013011700	CIP-006-3c	R5	Medium	
			SERC2011007999	CIP-006-3c	R6	Lower	
			SERC201000623	CIP-007-1	R1	Medium	
			SERC2011007873	CIP-007-1	R2	Medium	
			SERC2012010000	CIP-007-3a	R4	Medium	
			SERC2012009999	CIP-007-1	R5	Lower	
			SERC201000621	CIP-007-1	R6	Lower	
			SERC2011008271	CIP-007-3	R7	Lower	
			SERC2013012005	CIP-007-3a	R7	Lower	

CIP-002-1 R1[5]

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

> 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.
>
> ***

[5] The violations included in this Full Notice of Penalty cover more than one Version of the applicable Standard. The version indicated in the document reflects the version in effect at the time the violation began. The language of the Requirements involved remained the same in each version.

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 R1 provides:

The Responsible Entity shall comply with the following requirements of Standard CIP-002:

R1. Critical Asset Identification Method — The Responsible Entity shall identify and document a risk-based assessment methodology to use to identify its Critical Assets.

R1.1. The Responsible Entity shall maintain documentation describing its risk-based assessment methodology that includes procedures and evaluation criteria.

R1.2. The risk-based assessment shall consider the following assets:

R1.2.1. Control centers and backup control centers performing the functions of the entities listed in the Applicability section of this standard.

R1.2.2. Transmission substations that support the reliable operation of the Bulk Electric System.

R1.2.3. Generation resources that support the reliable operation of the Bulk Electric System.

R1.2.4. Systems and facilities critical to system restoration, including blackstart generators and substations in the electrical path of transmission lines used for initial system restoration.

R1.2.5. Systems and facilities critical to automatic load shedding under a common control system capable of shedding 300 MW or more.

R1.2.6. Special Protection Systems that support the reliable operation of the Bulk Electric System.

R1.2.7. Any additional assets that support the reliable operation of the Bulk Electric System that the Responsible Entity deems appropriate to include in its assessment.

CIP-002-1 R1 has a "Lower" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL).

This violation addresses multiple occurrences of noncompliance with CIP-002-1 R1.

SERC sent to URE an initial notice of a Compliance Audit (Compliance Audit). URE self-reported that it had not clearly documented the evaluation criteria in its risk-based assessment methodology (RBAM), which was used to identify its Critical Assets.

SERC reviewed the RBAM that was in place at the time and verified that it did not evaluate all of the criteria specified in R1. Specifically, the criteria did not require Critical Asset designation of generation blackstart resources that have been verified to meet system restoration needs. This resulted in the omission of two generation blackstart resource facilities that should have been identified as Critical Assets. The total capacity for the two generation facilities was 55 MW.

URE discovered this issue after evaluating a report from a consultant. URE revised its RBAM more clearly to identify the criteria for identification of generation blackstart resources that are considered Critical Assets.

While SERC was performing its assessment and determining the scope of the violation, the following additional occurrence of noncompliance was found.

The SERC audit team determined that a historical version of the RBAM failed to include sufficient criteria to identify all control centers and backup control centers with supervisory control of Critical Assets.

SERC reviewed the RBAM and determined that the URE RBAM did not have sufficient evaluation criteria to identify all Critical Assets. The RBAM criteria failed to indentify three generation control centers containing 20 Critical Cyber Assets (CCAs). URE revised its RBAM criteria. The resulting application of the criteria led to these assets being identified on the Critical Asset list as required in CIP-002 R2.

SERC determined that URE was in violation of CIP-002-1 R1.1 for failing to document the evaluation criteria in its RBAM used to identify its Critical Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE, through when the RBAM was revised.

SERC determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). The proper identification of Critical Assets is paramount to the reliable operation of the BPS. Critical Cyber Assets were at a greater risk of being compromised without the protective measures of the CIP Standards Compromised or inoperable Critical Assets could have caused the loss of monitoring and control of the BPS.

CIP-002-1 R2

CIP-002-1 R2 provides:

R2. Critical Asset Identification — The Responsible Entity shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary.

CIP-002-1 R2 has a "High" VRF and a "High" VSL.

URE self-reported a violation of CIP-002-1 R2 stating that URE did not identify all of its Critical Assets in its Critical Asset list.

URE discovered two Critical Assets that were not identified when applying its RBAM. URE discovered that the Critical Assets would need to be energized in order to connect a blackstart resource to another Critical Asset. The Critical Assets are part of the primary path used to energize a station switchyard, and therefore they should have been included on the Critical Asset list.

SERC determined that URE was in violation of CIP-002-1 R2 because it failed to develop a complete list of Critical Assets through the application of its RBAM.

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

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, if Critical Assets are destroyed, degraded, compromised, or otherwise rendered unavailable, they could affect the reliability or operability of the BPS. The Critical

Assets are at a substation in the preferred path used for initial system restoration as well as assisting in restoration in accordance with its system restoration plan. In the event that the Critical Assets were destroyed, degraded, compromised, or otherwise rendered unavailable, the BPS could be restored to a reliable point using other Critical Assets.

CIP-004-1 R4

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. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

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.

This violation addresses multiple occurrences of noncompliance with CIP-004-1 R4.

URE self-reported that an employee was granted access to a facility, which was not requested. The employee requested access to the NERC Substation Control Houses via URE's electronic access form. The employee was granted access to the wrong facility. The badge was coded to have access to two

different facilities, instead of the NERC Substation Control Houses. The initially requested access was added to the badge, but the incorrect access was not removed.

URE's CIP administrator discovered that the employee had been granted incorrect access. The employee's incorrect access was removed three days later.

While SERC was performing its assessment and determining the scope of the violation, two additional occurrences of noncompliance were found.

SERC sent URE an initial notice of a Compliance Audit. URE self-reported that it approved unescorted physical access to a facility with CCAs for an individual who should not have had such access. A contractor was mistakenly given unescorted access to a physical security perimeter (PSP) to which the contractor did not need access. The access was discovered and removed.

URE also self-reported that another employee was granted access to a facility, which was not requested. SERC determined that URE incorrectly gave an employee access to a PSP to which access was not needed. URE discovered and removed the access.

SERC determined that URE was in violation of CIP-004-1 R4 because it failed to maintain a list of personnel with authorized unescorted physical access to CCAs.

SERC determined the duration of the violation to be from when the first employee was granted access, through when the last access was revoked.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation was associated with 3 out of 169 employees. The employees never accessed the PSPs during the time access had been erroneously granted. Finally, the employees had completed cyber security training and Personnel Risk Assessments (PRAs).

CIP-005-3a R1.4

The purpose statement of Reliability Standard CIP-005-3a provides: "Standard CIP-005-3 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-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a 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).
>
> ****
>
> **R1.4.** Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005-3.

CIP-005-3a R1.4 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-005-3 R1.4 because URE failed to identify and to protect non-critical Cyber Assets within a defined Electronic Security Perimeter (ESP) pursuant to CIP-005-3. URE's Self-Report contained three separate occurrences of noncompliance.

The first occurrence was when URE installed a device that was connected via routable protocol to a second device that was already within an ESP. This action meant that the first device was now a Cyber Asset within the ESP. This device was used to provide a graphical representation of the substation. URE discovered that the device had not been afforded the required protections. URE disconnected the device from the ESP about a month later.

The second and third occurrences involved network switches at two separate ESPs. However, neither of the switches was afforded the required protections. According to URE, it discovered the issue and disconnected the devices from the about a month later.

SERC determined that URE was in violation of CIP-005-3 R1.4 because it failed to protect non-critical Cyber Assets within a defined ESP.

SERC determined the duration of the violation to be from when the first device was placed inside the ESP, through when the devices were disconnected from the ESPs.

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 protect all non-critical Cyber Assets within the ESP could result in vulnerabilities that allow an attacker to access or compromise systems within the ESP. However, the violation was for three non-critical Cyber Assets devices, all of which resided in ESPs with an intrusion detection system. Additionally, each device resided within a PSP within the same location, thereby reducing the risk to the BPS.

CIP-005-1 R2

CIP-005-1 R2 provides:

The Responsible Entity shall comply with the following requirements of Standard CIP-005-1:

R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).

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

R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.

R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.
R2.5.2. The authentication methods.
R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 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 document an adequate timeframe and justification for enabled ports and services during a scheduled cyber vulnerability assessment (CVA).

URE performed a review and analysis of compliance items resulting from its CVA. As part of its CVA process, URE performed penetration testing that required it to enable ports and services not otherwise required for operations or monitoring. During the review, URE discovered that the penetration testing process did not include an accurate timeframe for how long the penetration testing ports and services should remain open and a justification for that proposed timeframe.

URE also reported that 70 firewalls serving as electronic access points at each ESP had an access control rule-set, enabling penetration testing of both the access point and a network switch within the ESP. URE stated that the rule-set is required to perform the annual CVA. However, this rule-set remained in force longer than what was required for that CVA, meaning that URE had enabled ports and services not required for operations or monitoring. The penetration testing rule-set enabled access from two servers on URE's corporate network, and access to those servers was limited to three individuals.

URE's CVA program required the internal business units to complete a statement of work (SOW) with the internal IT security department prior to the start of the CVA. The program required the SOW to contain, among other things, a timeline of the assessment as agreed between the parties. URE's CVA SOWs at issue included proposed timeframes. Both CVA SOWs stated that the actual dates would be formalized and communicated prior to the start of the tests.

SERC found that one of the two CVA SOW at issue, URE stated that the access point rule-set would not be enabled for more than 45 days without approval from the business contacts. SERC found that URE did not formalize or communicate the start of the test, and the rule-set remained open for a period longer than 45 days. SERC also discovered that URE had enabled ports and services for penetration testing longer than was necessary for each annual CVA.

The rule-set at issue allowed unlimited access to all the ports of the ESP access point itself and to a network switch within the ESP. Only three individuals on the CVA team had access to the two servers required to utilize this access.

SERC determined that URE was in violation of CIP-005-1 R2 because it failed to enable and document only the ports and services required for operations and monitoring of Cyber Assets within the ESP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE, through when the CVA window ended.

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 rule-set enabled ports and services not needed for normal operation during an extended period of time , potentially providing unauthorized access to URE's Cyber Assets within the ESP, risking exposure of sensitive data and manipulation of applications or data. However, the rule-set enabled only two servers on URE's corporate network to access the access point and one switch within the ESP. Access through the access point was controlled by an access control list. These servers were used for the purpose of performing the annual CVA. Additionally, only three individuals, all of whom were part of URE's CVA team, had access to the two servers. The rule-set on the access point was limited and did not allow access to additional Critical Cyber Assets.

CIP-005-1 R3

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

This violation addresses multiple occurrences of noncompliance with CIP-005-1 R3.

On September 22, 2010, URE self-reported that it missed the manual log review that is required at least every 90 days by CIP-005-1 R3.2 when the automated control is not technically feasible. A

manual review should have been performed; however, the review did not occur within the required timeframe. .

SERC determined that URE had 13 dial-up access modems for which alerting was not technically feasible. These devices were included in a CIP-005-1 R3.2 Technical Feasibility Exception (TFE) submitted to SERC. Because alerting was not technically feasible, URE should have reviewed the modems' access logs. However, the review of the modems' access logs was completed 28 days after the review should have been completed. SERC determined that URE failed to review access logs for attempts at or actual unauthorized accesses at least every 90 calendar days.

While SERC was performing its assessment and determining the scope of the violation, three additional occurrences of noncompliance were found.

The SERC audit team reported a violation of CIP-005-1 R3 because URE failed to implement electronic or manual processes for monitoring access at certain access points to the ESP. While investigating the audit team's finding, URE identified 16 access points at 16 different ESPs (one access point at each ESP) that were not configured to monitor and to log access. URE has 29 ESPs in the SERC region. According to URE, it had failed to implement electronic or manual processes for monitoring the access points that were serial to internal protocol routable substation access points. SERC determined that URE failed to ensure that all access points have security status monitoring implemented due to insufficient processes and procedures.

URE self-reported that it missed the manual log reviews that are required at least every 90 days by CIP-005-1 R3.2 when the automated control is not technically feasible. SERC determined that URE replaced a manual log review process with an automated log review process to monitor and log dial-up access at access points to the ESP. However URE discovered that since the automated review process was implemented, the automated process was unsuccessful in consistently retrieving the access logs. URE implemented a new manual review process and submitted a TFE for the inability of the devices to perform automated alerting for attempts at unauthorized access. SERC determined that URE failed to review access logs for attempts at or actual unauthorized accesses at least every 90 calendar days, as required.

URE self-reported that it lost the capability of monitoring twenty-four hours a day, seven days a week at an ESP access point. According to URE, it discovered that an Intrusion Prevention System (IPS) sensor was offline, which resulted in the loss of IPS monitoring of network traffic to four ESPs. Due to a failure to act upon this discovery, the sensor was not restored for about a month.

SERC determined that URE was in violation of CIP-005-1 R3 because it failed to implement electronic or manual processes to monitor and log access at access points to the ESPs twenty-four hours a day, seven days a week.

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

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, failure to monitor access to the ESPs could result in unauthorized access attempts going undetected by URE. In addition, the failure to review access logs at least every 90 days limited URE's awareness of possible security issues. However, authentication and access controls were being performed at the access points, thereby reducing the risk to the BPS. While late, the manual log reviews did not reveal any reportable cybersecurity events.

CIP-005-3a R5

CIP-005-3a R5 provides:

> **R5.** Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005-3.
>
> > **R5.1.** The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
> >
> > **R5.2.** The Responsible Entity shall update the documentation to reflect the modification of the network or controls within ninety calendar days of the change.
> >
> > **R5.3.** The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

CIP-005-3a R5 has a "Lower" VRF and a "Severe" VSL.

URE self-reported that it failed to update documentation within 90 calendar days of a modification of the network.

According to URE, a Critical Asset underwent network modifications. The modifications were to upgrade the network by replacing devices from serial to internet protocol. URE discovered that the network drawing had not been updated to reflect the modifications. The documentation was updated 131 days after the modifications. There were 23 Cyber Assets within the ESP at this Critical Asset.

SERC determined that URE was in violation of CIP-005-3 R5 because it failed to update documentation within 90 calendar days of a modification of the network, as required.

SERC determined the duration of the violation to be from the date marking 91 days after the network modification, through when the documentation was updated.

SERC determined that this violation posed a minimal and not serious or substantial risk to the BPS. . The violation affected one drawing at one ESP and lasted for 41 days. There was no gap in availability of electronic or physical controls to the ESP during this time.

CIP-006-1 R1 and R1.1

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. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides in pertinent part:

> The Responsible Entity shall comply with the following requirements of Standard CIP-006:
>
> **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:
>
> > **R1.1.** Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

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

This violation addresses multiple occurrences of noncompliance with CIP-006-1 R1.

URE submitted a Self-Report because it found three occurrences where it failed to establish a completely enclosed "six-wall" border, or deploy and document alternative measures to control physical access to Cyber Assets within the PSP.

With regard to the first occurrence, RE discovered that an access panel located at the rear of the room could be pried open to gain access to the neighboring PSP. Upon discovery, URE posted contract security personnel at the location to monitor physical access. URE fastened metal straps over the access panel opening to mitigate and completed the work on the same day as the discovery. URE performed a system-wide inspection of all URE PSPs and found that there were no additional access panels that presented the same vulnerability.

With regard to the second occurrence, URE discovered that a service elevator could be opened onto the second floor of the PSP after being called by someone with an authorized badge. This could have allowed an unauthorized person riding on the elevator to enter the PSP. URE also found that the elevator cab had an access panel on the roof that was not being monitored for unauthorized access. URE reprogrammed the elevator to disable the second floor call button to alleviate the issue.

Finally, at a different PSP, URE discovered an opening in the PSP's walls that exceeded the maximum allowable size of 96 square inches. The opening was a cable trough entering the PSP at ground level. URE posted security personnel at the area where the opening was discovered until it installed metal barriers in the opening on the same day as the discovery. SERC determined that URE failed to establish completely enclosed six-wall borders or to deploy and document alternative measures used to control physical access to PSPs.

While SERC was performing its assessment and determining the scope of the violation, the following additional occurrence of noncompliance was found.

URE self-reported that it discovered an opening in a PSP's suspended ceiling that exceeded the maximum allowed opening size of 96 square inches. This opening had previously been protected by a metal strap. However, the strap had been severed. URE was unable to determine the date, time, or reason the metal strap was severed.

SERC determined that URE was in violation of CIP-006 R1.1 because it failed to establish completely enclosed six-wall borders or to deploy and document alternative measures used to control physical access to PSPs.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS.

As to the first occurrence of noncompliance, the PSP was contained within a protected building secured by closed circuit television, contract security personnel, and badge access entry points, and was manned twenty-four hours a day, seven days a week by URE's personnel. The mechanical room is limited to facilities personnel and is located within an operations center building that offers on-site contract security and card-access controlled building access, and the location is manned twenty-four hours a day, seven days a week by URE personnel. Also, access to the panel was limited by heavy equipment.

As to the second occurrence, the elevator at issue was a service elevator that was not normally used, thus limiting the opportunities for the elevator to be called to the second floor.

As to the third occurrence, the PSP was surrounded by security fencing, displayed warning signage, and was protected by a gate where access was limited to authorized personnel.

As to the last occurrence, the PSP was completely enclosed by a barbed wire fence, and access was restricted by a locked gate.

CIP-006-1 R1

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

SERC sent URE an initial notice of a Compliance Audit. URE self-reported that it had discovered an undocumented opening in a PSP wall at a control center.

URE began and completed a construction project to remove a security fire gate, a motor, and a frame. This created a two-foot wide by three-foot tall opening in the PSP. The opening was not easily visible since it was behind a locked closet and above a suspended ceiling. The violation was discovered while preparing for the Compliance Audit. The PSP at issue contained 42 CCAs at the time of the violation.

SERC determined that URE was in violation of CIP-006-1 R1 because it failed to maintain a physical security plan to ensure that all Cyber Assets within an ESP reside within an identified PSP.

SERC determined the duration of the violation to be from the date the PSP was not completely enclosed, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failing to enclose the PSP completely within a six-wall border could have allowed unauthorized physical access to the CCAs and the issue was not discovered until 659 days after it began. However, the opening was behind a locked electric closet door and above a suspended drywall ceiling. Access to the opening was limited due to conduit, steel support bracing, and steel wall studs in the area. The CCAs are located in a separate area within the PSP, and access is restricted by an additional card key reader. Additionally, the area of the building where the opening existed was regularly patrolled by corporate security.

CIP-006-3c R5 (SERC2012011337)

CIP-006-3c 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-008-3. 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-006-3c R5 has a "Medium" VRF and a "Severe" VSL.

URE self-reported that it failed to monitor physical access at all access points to the PSP twenty-four hours a day, seven days a week.

SERC determined that URE personnel completed a physical security inspection at a PSP. During this inspection, URE discovered that an exit-only door did not alarm during the hold-open and the forced-open operational tests. The door alarm was repaired the same day, and the cause was found to be a

defective processor board. The PSP contained two CCAs and 31 non-critical Cyber Assets within the ESP. According to URE, it completed an assessment of its other PSPs in and found no additional processor board failures.

SERC determined that URE was in violation of CIP-006-3 R5 because it failed to implement the technical controls for monitoring physical access at all access points to the PSPs twenty-four hours a day, seven days a week.

SERC determined the duration of the violation to be from the last known date the alarm was functioning, through when the alarm was repaired.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation occurred on one door at a PSP that was exit-only, which could not be opened externally. The door was accessible only to personnel with approved unescorted access to the PSP or escorted visitors who had previously gained authorized access via other entry access points. Personnel would only have been able to exit through this door.

CIP-006-3c R5 (SERC2013011700)
CIP-006-3c R5 has a "Medium" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of noncompliance with CIP-006-3c R5.

URE submitted a Self-Report to SERC stating that it failed to implement the technical controls for monitoring physical access at all access points to the PSP and for failing to review and respond to unauthorized access attempts immediately.

URE discovered that alarms to the security monitoring console were not being delivered in a timely manner. The system was malfunctioning, and alarms related to unauthorized access attempts were delayed. The delay lasted from 9:54 a.m. to 3:00 p.m. URE discovered that the monitoring system was experiencing software errors due to the upgrade of the system operating system. Therefore, SERC determined that URE failed to implement the technical controls for monitoring physical access at all access points to the PSPs.

While SERC was performing its assessment and determining the scope of the violation, the following six additional occurrences of noncompliance were found

URE self-reported that it discovered that there was no record of response for three unauthorized access attempts. The attempts occurred on the same day. At 3:27 p.m. and 3:28 p.m., an employee

attempted to gain access to three PSP doors. The individual was denied access, and URE received the appropriate alarm. However, the security console operator failed to review the alarm and respond accordingly. URE confirmed that the employee had a current PRA, the required cybersecurity training, and was authorized for physical access to the PSP. The employees badge had been incorrectly deactivated.

URE self-reported that it was not able to monitor and respond to NERC alarms at a PSP due to a loss of network communications. SERC determined that without network connectivity, the field micro-controller, located at the PSP, was unable to communicate with the central server. Network communications were lost at 7:18 a.m. and restored at 8:34 a.m. the same day. The communications link was again interrupted at 6:16 p.m. and restored at 6:53 p.m. the same day. The network outages were caused by maintenance work at the substation control house. The micro-controllers and the door access control components continued to operate under battery backup during the incident. SERC determined that badge activity logs and alarms were cached and delivered to the central server when communications were restored. URE reviewed the logs and alarms after the network was restored and confirmed there were no door forced-open alarms, door held-open alarms, or unauthorized access attempts. Therefore, SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

URE self-reported that it experienced software errors between the physical access control system (PACS) server and the monitoring console workstations. URE reported that from 9:14 a.m. to 9:34 a.m. the same day, it took the primary and the backup PACS servers offline to correct the software errors. The servers were again taken offline for maintenance at 10:04 a.m., and brought back online at 10:57 a.m. the same day. During these outages, URE was unable to monitor door alarms, as required. The alarms were being cached (temporarily stored) at the local field devices but did not post to the operator console until the servers were operational. Therefore, SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week. URE self-reported that it was unable to monitor and respond to alarms for all of URE's PSPs. The workstation console, which is used to monitor the PACS alarms for PSP access points, encountered a system problem which caused the monitoring console to stop receiving alarms from approximately 6:24 p.m. the PACS server. Therefore, SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week. According to URE, the underlying cause of the issue was a computer communications or software error between the monitoring console and

URE reported that, at 7:03 p.m. URE observed that the PACS had malfunctioned and had not received any alarms or badge activity since 4:51 p.m. At 8:38 p.m., the system was restored. URE reported that the underlying cause of the issue was a computer communications or software error between the

monitoring console and the PACS server. Therefore, SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

URE reported that at 3:36 a.m., there was a communication failure with the primary PACS, which rendered the monitoring console unable to display alarm activity for all of URE's PSPs. According to URE, the primary system shutdown at 3:39 a.m., due to a lack of network connectivity and an emergency trouble ticket was submitted to the incident ticketing system. At 5:30 a.m., URE began monitoring security alarms utilizing the backup PACS server. At 1:08 p.m., the primary PACS application was restored and monitoring resumed using the primary PACS server. Therefore, SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

SERC determined that URE was in violation of CIP-006-3c R5 because it failed to implement the technical controls for monitoring physical access at all access points to the PSPs twenty-four hours a day, seven days a week. and to review unauthorized physical access attempts immediately.

SERC determined the duration of the violation to be from the date URE experienced the first issue with the logging and monitoring software, 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, unauthorized access to the PSPs could have occurred and gone undetected as a result of these issues. However, the PSP access points were operating as intended and provided audible alarms at the applicable locations. Once the system was operational, alarms were received, and URE verified that there were no unauthorized access attempts during the time periods in question. Also, the functionality of the card readers at the PSPs was not diminished by the issues described above; all still restricted access to only authorized individuals.

CIP-006-3c R6

CIP-006-3c R6 provides:

> **R6.** Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

• Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

• Video Recording: Electronic capture of video images of sufficient quality to determine identity.

• Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

CIP-006-3c R6 has a "Lower" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of noncompliance with CIP-006-3c R6.

SERC sent URE an initial notice of Compliance Audit. URE self-reported a violation of CIP-006-3c R6 because it failed to maintain real-time manual logging of the access to the PSP.

SERC determined that URE's automated physical PACS failed and lost the capability to monitor and to log access to the PSP. The PACS utilizes a card reader that logs card keys uniquely coded for authorized user access. The failure occurred approximately five hours into a scheduled station outage due to a weak battery. In addition to the card reader, URE maintains a logbook or sign-in sheet at the PSPs for the manual logging of personnel. During the period of the card reader failure, the doors failed close and access could only be gained with authorized keys. Four URE employees entered the PSP but did not sign in to the log book. The facility was returned to service later the same day along with the PACS. SERC determined that URE was in violation of CIP-006-3c R6 because it failed to log physical access for individuals entering PSPs twenty-four hours a day, seven days a week.

While SERC was performing its assessment and determining the scope of the violation, the following additional occurrence of noncompliance was found.

URE self-reported that it allowed an employee to access a PSP without logging such access. SERC learned that an employee returning from a medical leave of absence tried to access a PSP. However, due to deactivation, the employee was unable to log access into the PSP. URE's procedures required employees without an authorized ID badge to manually sign in and out of the PSP and to have an authorized escort at all times. When the employee's badge failed to open the protected door, the employee was granted access by another employee; however, the employee did not sign the log book.

URE became aware that an employee's badge had not been reactivated. That same day, the employee's badge was reactivated.

SERC determined that URE was in violation of CIP-006-3c R6 because it failed to log physical access for individuals entering PSPs twenty-four hours a day, seven days a week.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The unlogged access was limited to one instance each for five employees. All of the employees involved in these instances of noncompliance had current PRA and cybersecurity training as required by CIP-004 R2 and R3.

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). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

The Responsible Entity shall comply with the following requirements of Standard CIP-007 for all Critical Cyber Assets and other Cyber Assets within the Electronic Security Perimeter(s):

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

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

This violation addresses multiple occurrences of noncompliance with CIP-007-1 R1.

URE self-reported that its laptops connected to the substation devices within an ESP were not tested, as required by CIP-007 R1. URE discovered that contractors connected their laptops to substation devices within two ESPs. SERC determined that at one of the ESPs, the laptops were connected before the mandatory and enforceable date of this Standard; therefore, the issue only occurred at one ESP. The contractors' laptops had not been tested in accordance with CIP-007-1 R1 before being connected to the ESP.

SERC determined that the two contractor laptops were connected to the ESP in order to implement the necessary relay settings required to replace two breakers. Therefore, SERC determined that URE failed to ensure that new Cyber Assets within the ESP did not adversely affect existing cybersecurity controls.

While SERC was performing its assessment and determining the scope of the violation, the following additional occurrence of noncompliance was found.

SERC sent URE an initial notice of a CIP Compliance Audit. The SERC audit team determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within an ESP did not adversely affect existing cybersecurity controls.

SERC determined that 142 CCAs and 169 Cyber Assets had not been tested in accordance with its test procedures. SERC determined that URE failed to ensure that new Cyber Assets and existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls. Therefore, SERC determined that URE was in violation of CIP-007-1 R1 because it failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within ESPs did not adversely affect existing cybersecurity controls.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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, if significant changes are not tested to verify the effect they have on the security controls, security vulnerabilities can be introduced without the knowledge of URE and without appropriate compensating or mitigating measures being taken. These security vulnerabilities could allow unauthorized personnel the ability to disrupt the operation of the Cyber

Asset or gain command and control over the asset itself. However, URE had implemented two-factor authentication at the ESP access points, and the contractors' laptops were only serially connected.

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.

This violation addresses multiple occurrences of noncompliance with CIP-007 R2.

URE self-reported that it was unable to confirm that its laptops connected to the substation devices within the ESPs comply with CIP-007-1 R2 ports and services processes for Cyber Assets within the ESP.

URE had a process to ensure that only those ports and services required for normal and emergency operations were enabled. SERC determined that two contractor laptops were connected to the ESP and utilized to implement the necessary relay settings required to replace two breakers.

The SERC audit team determined that URE failed to disable ports and services not needed for normal and emergency operations. SERC determined that 64 Cyber Assets had ports and services enabled that were not needed for normal or emergency operations; therefore, they should have been disabled. According to URE, the processes for maintaining ports and services baselines did not adequately identify the ports and services required for normal and emergency operations.

Therefore, SERC determined that URE was in violation of CIP-007-1 R2 because it failed to disable ports and services not needed for normal and emergency operations.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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, if unused ports and services are left open, unauthorized individuals or malware could use these ports to disrupt operations or gain unauthorized command and control of the affected Cyber Assets. This could have resulted in CCAs being compromised or rendered inoperable. However, URE had implemented an intrusion detection system (IDS) within the ESPs, which should provide additional notification to URE employees regarding possible malicious activity.

CIP-007-3a R4

CIP-007-3a 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-007-3a R4 has a "Medium" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of noncompliance with CIP-007-3a R4.

URE self-reported that it failed to use anti-virus software and other malicious software prevention tools on one CCA. URE discovered that a technician failed to issue a command required by a configuration change procedure, resulting in the failure of the malicious software prevention tool on

one CCA. SERC determined that the affected CCA was a station data manager used to render a visible representation of the substation configuration. This device uses whitelisting software, which blocks all commands that are not explicitly included on the list. URE re-enabled the malicious software prevention tool on the CCA. This occurrence affected one device out of 17 at the substation. Therefore, SERC determined that URE failed to use anti-virus software and other malicious software prevention tools, where technically feasible.

While SERC was performing its assessment and determining the scope of the violation, the following two additional occurrences were found.

URE self-reported that it discovered that a TFE should have been submitted for five Cyber Assets at the time they were commissioned because they did not support anti-virus or malware prevention tools. SERC determined that the Cyber Assets were programmable automation controllers. URE submitted a TFE for these devices. Therefore, SERC determined that URE failed to file a TFE related to its inability to install malware and anti-virus protection tools on the identified Cyber Assets.

URE self-reported that during a review, it discovered that a TFE should have been submitted for certain Cyber Assets at the time they were commissioned because they did not support anti-virus or malware prevention tools. SERC determined that five Cyber Assets were involved. The Cyber Assets were data commissioning devices that were added to production. SERC determined that URE failed to file a TFE related to URE's inability to install malware and anti-virus protection tools on the identified Cyber Assets.

Therefore, SERC determined that URE was in violation of CIP-007-3a R4 because it failed to use anti-virus software and other malicious software prevention tools, where technically feasible.

SERC determined the duration of the violation to be from the date URE failed to implement the malicious software prevention tool, through when URE submitted the last required TFE.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The station data manager did not have malicious software prevention tools implemented for 31 days, and user access to the station data manager was limited. Additionally, there were no viruses or unexpected whitelisted applications discovered. URE had compensating measures in place at the time of commissioning regarding the Cyber Assets for which malware and anti-virus protection tools could not be installed. There were 10 Cyber Assets out of 1213 Cyber Assets (less than one 1%) that did not have a TFE submitted.

CIP-007-1 R5

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 "Lower" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of noncompliance with CIP-007-1 R5.

URE self-reported that it failed to generate logs of sufficient detail to create historical audit trails for access to shared accounts and failed to review access privileges of all users annually. SERC determined that the audit trails for user account access activity were not being generated for 31 shared accounts that were accessed by a total of 68 users. These shared accounts accessed 25 CCAs and 12 non-critical Cyber Assets within the ESP. With regard to annual user account access verification, URE did have a process in place but did not follow it. URE failed to perform the annual reviews for four years. . Therefore, SERC determined that URE failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access, as required.

While SERC was performing its assessment and determining the scope of the violation, the following additional occurrence was found.

URE self-reported that it failed to submit a TFE for devices that could not enforce the password complexity requirement.

SERC determined that URE commissioned five data communications devices that could not meet the password complexity requirement. Specifically, these devices could not accept "special" characters in the password. While the compensating measures were in effect at the time of commissioning, URE did not file the TFE within the required timeframe. SERC determined that URE failed to submit a TFE on the identified devices' inability to require and use "special" characters, as required. SERC determined that URE failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access, as required.

SERC determined that URE was in violation of CIP-007-1 R5 because it failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

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, URE's failure to log shared user account access activity could allow suspicious or malicious activities to go undiscovered. Failing to review access privileges could result in individuals having unauthorized access or access to Cyber Assets that they should no longer have. Additionally, if password complexity is not enforced, the passwords are more likely to be successfully compromised. However, the shared accounts were restricted to users who have had PRAs and cybersecurity training. Compensating and mitigating measures for password complexity (excluding special characters) were in place at the time the devices were commissioned.

CIP -007-1 R6

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.

This violation addresses multiple occurrences of noncompliance with CIP-007-1 R6.

URE self-reported that a TFE should have been filed for some devices within an ESP. SERC determined that there were 282 Cyber Assets that were unable to log and report security events as prescribed in CIP-007-1 R6 that did not have a TFE. These devices included relays, modems, communications processors, digital fault recorders, Ethernet switches, port servers, and a real-time automation controller. The devices lacked the capability to perform security status logging and reporting, and URE lacked the infrastructure that would enable URE to evaluate the data if it was available.

While SERC was performing its assessment and determining the scope of the violation, the following two additional occurrences were found.

URE self-reported that it discovered that a TFE should have been filed for five cyber assets at the time they were commissioned because the devices did not support monitoring or logging of system events related to cybersecurity. URE commissioned five discrete programmable automation controllers within ESPs that could not perform security status monitoring, as required.

URE self-reported that during a review, it discovered Cyber Assets for which a TFE was required because of their inability to support security status monitoring. SERC determined that URE commissioned five data communications devices within an ESP that could not perform security status monitoring.

SERC determined that URE was in violation of CIP-007-1 R6 because it failed to file TFEs on identified devices' inability to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to implement security status monitoring for its Cyber Assets within the ESPs could have resulted in a security breach being undetected. However, the TFE compensating measures had been implemented before or at the time the devices were commissioned.

CIP-007-3 R7

CIP-007-3 R7 provides:

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

CIP-007-3 R7 has a "Lower" VRF and a "Severe" VSL.

SERC sent URE an initial notice of a CIP Compliance Audit. The SERC audit team reported that URE failed to implement formal methods, processes, and procedures for the disposal or the redeployment of all Cyber Assets within the ESP. Specifically, three non-critical Cyber Assets had been redeployed or decommissioned without erasing the data storage media to prevent the unauthorized retrieval of sensitive cybersecurity or reliability data.

SERC determined that one of the Cyber Assets was a server used for storage management. While URE's procedure requires the server's hard drive to be wiped or destroyed, URE's personnel did not

follow the documented procedures and failed to erase the data storage media prior to its redeployment. The other two Cyber Assets were a router and a switch. URE personnel did not follow the documented procedures and failed to erase the data storage media prior to its redeployment.

SERC determined that URE was in violation of CIP-007-3 R7 because it failed to follow the implemented formal methods, processes, and procedures for the disposal or redeployment of all Cyber Assets within the ESP.

SERC determined the duration of the violation to be from the date the first redeployment occurred, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The Cyber Assets in question contained no data other than IP addresses and configuration settings. In addition, URE had a process in place for the disposal or the redeployment of Critical Assets within the ESP but failed to follow it for the non-critical Cyber Assets at issue.

CIP-007-3a R7

CIP-007-3a R7 provides:

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

CIP-007-3a R7 has a “Lower” VRF and a “Severe” VSL.

URE submitted a Self-Report to SERC that it was in violation of CIP-007-3a R7 because it failed to follow the established processes for moving production equipment from an ESP to a non-ESP.

URE moved two CCAs that provided time information to the Energy Management System (EMS) from the ESP, in which they resided, to a non-ESP network in order to perform device reconfiguration. The two devices required reconfiguration due to their failure to provide correct time information to the EMS. Removing these devices from the ESP and connecting them to a non-ESP network constituted redeployment. URE connected the devices to the non-ESP network, replaced the existing IP address with a non-ESP IP, performed the reconfiguration, and then returned the devices to the ESP network without following URE's redeployment process.

SERC determined that URE's CCA disposal or redeployment process did not specifically address the type of asset at issue and URE did not follow the process for redeployment for its devices. URE failed to remove the configuration data from the device prior to its removal from active service, as required by its redeployment process.

SERC determined that URE was in violation of CIP-007-3a R7 because it failed to establish and implement formal methods, processes, and procedures for redeployment of Cyber Assets within the ESP.

SERC determined the duration of the violation to be from the date the devices were removed from the CCA, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The time devices supply time information and support no other vital function to the CCAs. The technician performing the change had completed the required cybersecurity training and had a PRA. The Cyber Assets are firmware based devices with no third-party applications installed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC determined that URE's previous violation of CIP-004-1 R4 was considered an aggravating factor in the penalty determination;
2. SERC did not consider URE's remaining violation history an aggravating factor in the penalty determination

3. URE self-reported some of the violations, which was considered a mitigating factor in the penalty determination;
4. URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violations, which SERC considered a mitigating factor;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violation of CIP-002-1 R1 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
8. URE agreed to complete several above-and-beyond mitigating measures, as described below; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

In addition to the monetary penalty of two hundred fifty thousand dollars ($250,000), URE agreed to complete several above-and-beyond mitigating actions, which are described below:

1. URE completed an analysis correlating the U.S. Department of Energy Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)[6] 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 ("Evaluation"). The Evaluation consisted of URE3'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.

[6] 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 URE3 with the effort to utilize internal controls to maintain compliance with the CIP Standards and ensure reliability of the BPS.

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 two hundred fifty thousand dollars ($250,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[7]

CIP-002-1 R1 and CIP-002-1 R2
URE's Mitigation Plan to address its violations of CIP-002-1 R1 and CIP-002-1 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 these violations is designated as SERCMIT006976-3 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revise its RBAM;
2. update its CCA; and
3. update the CCA list, as applicable.

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

CIP-004-1 R4
URE's Mitigation Plan to address its violation 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 is designated as SERCMIT004516-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the incorrect access;
2. review and update the current procedures for granting and revoking access at an enterprise level; and

[7] *See* 18 C.F.R § 39.7(d)(7).

3. train all applicable personnel on the procedures.

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

CIP-005-3a R1

URE's Mitigation Plan to address its violation of CIP-005-3a R1 was submitted to SERC on, stating it had been completed on. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT-008975 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. disconnect the devices from the ESPs;
2. develop and distribute a communication to applicable personnel regarding the classification of non-critical Cyber Assets within an ESP and their required protection; and
3. develop and distribute a procedure that establishes a protocol for communicating information about Cyber Assets to the business unit responsible for the protection of the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 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 is designated as SERCMIT009607-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revise the SOW to include additional verbiage stating how long firewall rules will remain open for the purpose of performing CVAs;
2. allow the firewall rules to enable access to perform scanning from two CVA virtual servers that are on the internal corporate network which have static IP addresses assigned to them;
3. change configuration to require that in order for a user to gain access to the virtual servers, a user must have an active directory account enabled on the virtual server. Access is limited to five individuals on URE's vulnerability assessment team; and
4. communicate these changes to URE's business unit.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R3

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 is designated as SERCMIT004764-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop and implement a script for a data export to a common server utilizes a log aggregation tool for the review of logs and the issue of alerts;
2. implement monitoring at the access points;
3. provide training to all personnel involved in ESP monitoring;
4. implement a procedure to manually collect device logs and review them within 90 days for those devices where automated control is not technically feasible;
5. submit the necessary TFE;
6. complete a failover to restore the IPS sensor; and
7. amend the monitoring procedure and communicate the changes to the applicable personnel.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-3a R5

URE's Mitigation Plan to address its violation of CIP-005-3a 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 is designated as SERCMIT008632 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the drawing at issue;
2. implement weekly meetings in order to review site changes and the required updates to the documentation; and
3. distribute an awareness bulletin to the transmission business unit reminding personnel that documentation, including the subject drawings, must be updated within ninety calendar days following changes to a site.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R1 and R1.1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009492 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. fasten metal straps over the access panel opening on the secured side of the PSP to complete the six wall border;
2. update the six wall criteria physical security guidelines with criteria for service elevators within a PSP;
3. provide and communicate the changes to applicable personnel;
4. install metal barriers in the cable troughs to complete the six wall border;
5. develop a PSP inspection process training and trained applicable personnel;
6. install a steel plate across the entire opening in the wall of the utility room to complete the six wall border;
7. implement a PSP change control process for work being conducted in and around the PSP and trained applicable personnel on the new process;
8. establish a project team and developed the scope of work for installation of door contacts on the service elevator; and
9. complete the service elevator project and updated the Physical Security Plan.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 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 is designated as SERCMIT009269 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the six wall border;

2. implement a process for notification and oversight of construction activities in or around PSPs;
3. review awareness training for PSPs and update, as needed; and
4. provide PSP awareness training to the appropriate personnel.

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

CIP-006-3c R5 (SERC2012011337)

URE's Mitigation Plan to address its violation of CIP-006-3c 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 is designated as SERCMIT009204-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace the processor defective board and perform operational testing to verify operation; and
2. perform an assessment of its other PSPs. URE found no additional processor board failures.

URE certified on June 3, 2013 that the above Mitigation Plan requirements were completed on.

CIP-006-3c R5 (SERC2013011700)

URE's Mitigation Plan to address its violation of CIP-006-3c 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 is designated as SERCMIT009865-1 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 alarms received on to determine if any other alarms were not responded to in accordance with CIP-006 R5;
2. report the incident to the console operator supervisor for follow-up;
3. discipline the employee at issue;
4. have the employee complete the NERC certification re-training and exam;
5. issue an email to the contracted alarm monitoring supervisor to request a process change for the alarm reviews;

6. update the applicable procedure to reflect this change;
7. issue an email to all console operators and supervisors providing the link to the new procedure;
8. restore network connectivity;
9. review the alarm logs and found no forced open, hold open or unauthorized access attempts during the loss of network communications;
10. implement a PSP change control process for work being conducted in and around the PSP;
11. conduct training on the new process with the applicable personnel;
12. correct the error messages;
13. conduct an operational test to generate a "Held Open" alarm at a PSP access point;
14. restart the application in order to restore monitoring to an operational state;
15. perform several troubleshooting techniques to resolve the communications error;
16. upgrade and implemented a newer version of the software involved;
17. update the Physical Security Plan to reflect the upgraded software;
18. update the notification process;
19. replace the defective processor board on the door and performed operational testing to confirm proper operation;
20. reconfigure the primary and backup PACS servers by increasing the number of failed pings from one to six for a total of sixty seconds of no connectivity before shutting down;
21. review and acknowledged all of the alarms from the outage;
22. update its standard operating procedure to include instructions for accessing the browser uniform resource locators (URLs) for the primary server and the backup server; and
23. communicate the change in procedure to applicable personnel.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R6

URE's Mitigation Plan to address its violation of CIP-006-3c 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 is designated as SERCMIT006912-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. counsel personnel regarding the existing procedure and protocol; and
2. include an article within a quarterly communication addressing physical security access requirements.

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

CIP-007-1 R1 and R2

URE's Mitigation Plan to address its violations of CIP-007-1 R1 and R2 was submitted to SERC, stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for these violations is designated as SERCMIT004632-5 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. disallow contractors to connect non-URE laptops to CCAs;
2. conduct PRAs and cybersecurity training for all contractors;
3. update the CIP-007 R1 procedures and processes and train applicable personnel;
4. disable all of the ports and services that were not needed for emergency and normal operations;
5. update the procedures and processes used to manage ports and services;
6. update the change control and testing process to increase the visibility of changes to ports and services; and
7. apply the updated processes and procedures to the Cyber Assets identified by the current violation within URE's ESPs in order to generate baselines with justifications.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-3a R4

URE's Mitigation Plan to address its violation of CIP-007-3a 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 is designated as SERCMIT009195-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. re-enable the malicious software prevention tool on the CCA;
2. communicate directly with the technician support group that failed to follow the procedures;
3. submit the necessary TFEs; and
4. develop and implement a questionnaire to be used when assessing Cyber Assets for TFEs.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009333 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify systems with shared accounts;
2. verify that the passwords have been changed within the past year;
3. verify that each system with shared accounts has a logging mechanism to provide audit trail evidence at the individual user level;
4. implement processes to provide audit trail evidence;
5. implement a TFE checklist to assets for TFE applicability before CCAs are put into production; and
6. add the TFE checklist to existing CCA design and replacement processes and train applicable personnel.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R6

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 is designated as SERCMIT004049-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. file the required TFEs;

2. implement a TFE assessment checklist and communicate its creation to applicable personnel;
3. incorporate the use of the TFE checklist when evaluating the possible redesign or replacement of CCAs; and
4. train applicable personnel on the use of the TFE checklist.

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

CIP-007-3 R7

URE's Mitigation Plan to address its violation of CIP-007-3 R7 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 is designated as SERCMIT006918-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. erase or decommission the devices at issue;
2. review and update the asset disposal and redeployment procedures as necessary; and
3. create a change control and asset disposal and redeployment specific training program and train all applicable personnel.

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

CIP-007-3a R7

URE's Mitigation Plan to address its violation of CIP-007-3a R7 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009338 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. determine the feasibility of implementing the technical control, which will lock down all switch network ports;
2. develop an implementation plan for deploying the technical control;

3. compile a listing of applicable personnel to determine who will receive the communication for the control that is being developed;
4. email applicable personnel regarding the technical control solution which will be sent via email to the affected personnel; and
5. deploy the switch network port lock down solution into production by setting the ports to either admin or locked based on input from the subject matter expert.

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[8]

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,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a two hundred fifty thousand dollar ($250,000) 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. SERC determined that URE's previous violation of CIP-004-1 R4 was considered an aggravating factor in the penalty determination;
2. SERC did not consider URE's remaining violation history an aggravating factor in the penalty determination;

[8] *See* 18 C.F.R. § 39.7(d)(4).
[9] *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).

3. URE self-reported some of the violations, which was considered a mitigating factor in the penalty determination;
4. URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violations, which SERC considered a mitigating factor;
6. URE agreed to complete several above-and-beyond mitigating measures, as described above;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. The violation of CIP-002-1 R1 posed a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred fifty thousand dollars ($250,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be Included as Part of this Notice of Penalty

a) Settlement Agreement by and between SERC and URE, included as Attachment a;
b) Disposition Documents[10]
c) Record documents for the violation of CIP-002-1 R1, included as Attachment c:
    1. URE's Source Documents;
    2. URE's Mitigation Plan designated as SERCMIT006976-3;
    3. URE's Certification of Mitigation Plan Completion;
d) Record documents for the violation of CIP-002-1 R2, included as Attachment d:
    1. URE's Source Document;

[10] The Disposition Document serves as SERC's Verification of Mitigation Plan Completion for all the below violations.

2. URE's Mitigation Plan designated as SERCMIT006976-3;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Documents;
2. URE's Mitigation Plan designated as SERCMIT004516-2 ;
3. URE's Certification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-005-3a R1, included as Attachment f:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008975;
3. URE's Certification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-005-1 R2, included as Attachment g:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009607-1;
3. URE's Certification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-005-1 R3, included as Attachment h:

1. URE's Source Documents;
2. URE's Mitigation Plan designated as SERCMIT004764-2;
3. URE's Certification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-005-3a R5, included as Attachment i:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008632;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009442;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009269;
3. URE's Certification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-006-3c R5, included as Attachment l:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009204-1;
3. URE's Certification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-006-3c R5, included as Attachment m:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009865-1;
3. URE's Certification of Mitigation Plan Completion;

n) Record documents for the violation of CIP-006-3c R6, included as Attachment n:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT006912-1;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT004632-5;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Documents;
2. URE's Mitigation Plan designated as SERCMIT004632-5;
3. URE's Certification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-007-3 R4, included as Attachment q:

1. URE's Source Documents;
2. URE's Mitigation Plan designated as SERCMIT009195-1;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009333 ;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT004049-1;
3. URE's Certification of Mitigation Plan Completion;

t) Record documents for the violation of CIP-007-3 R7, included as Attachment t:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT006918-1;
3. URE's Certification of Mitigation Plan Completion;

u) Record documents for the violation of CIP-007-3a R7, included as Attachment u:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT009338;
3. URE's Certification 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 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 Andrea B. Koch* Director, Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704)940-8219 (704) 357-7914 – facsimile	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 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

akoch@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.	

PRIVILEGED AND CONFIDENTIAL INFORMATION
HAS BEEN REMOVED FROM THIS PUBLIC VERSION

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
Unidentified Registered Entity

Attachments