PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2013

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity (URE), FERC Docket No. NP14-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] of CIP-002-1 R3; CIP-002-3 R3; CIP-004-1 R3, R4; CIP-004-3 R2.3, R4; CIP-004-3a R4.1; CIP-005-1 R1.1, R2.2, R4.5, R5.2; CIP-006-1 R1.1, R1.8, R3, R6; CIP-006-2 R2.1; CIP-006-3c R1.6, R4, R5; CIP-007-1 R1, R2, R3, R4.2, R5.3, R6.4, R7, R7.3, R8.4; and CIP-009-1 R1. According to the Settlement Agreement, URE admits the violations and has agreed to the assessed penalty of three hundred and fifty thousand dollars ($350,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

---

[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.

Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC200900394, SERC200900399, SERC200900402, SERC201000573, SERC201000575, SERC201000576, SERC200900599, SERC201000609, SERC201000611, SERC201000612, SERC201000613, SERC201000614, SERC201000615, SERC201000616, SERC201000617, SERC201000618, SERC201000619, SERC201000620, SERC2012010717, SERC2012010718, SERC2012010953, SERC2012010954, SERC2012010998, SERC2012011007, SERC2012011008, SERC2012011117, SERC2012011161, SERC2012011433, SERC2012011434, SERC2012011435, SERC2012011437, SERC2013011699, SERC2013011706, SERC2013012206, SERC2013012431, SERC2013012710, and SERC2013012712 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 16, 2013, by and between SERC and URE. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corpor-ation	URE	NOC - 2240	SERC200900394	CIP-002-1	R3	High	$350,000
			SERC200900399	CIP-004-1	R4	Lower	
			SERC200900402	CIP-009-1	R1	Medium	
			SERC201000573	CIP-007-1	R7	Lower	
			SERC201000575	CIP-007-1	R1	Medium	

			SERC201000576	CIP-007-1	R3	Lower	
			SERC200900599	CIP-004-1	R3	Lower	
			SERC201000609	CIP-002-1	R3	High	
			SERC201000611	CIP-005-1	R2; R2.2	Medium	
			SERC201000612	CIP-005-1	R4; R4.5	Medium	
			SERC201000613	CIP-005-1	R5; R5.2	Lower	
			SERC201000614	CIP-006-1	R1; R1.8	Lower	
			SERC201000615	CIP-006-1	R6	Medium	
			SERC201000616	CIP-007-1	R1	Medium	
			SERC201000617	CIP-007-1	R2	Medium	
			SERC201000618	CIP-007-1	R5; R5.3.3	Medium	
			SERC201000619	CIP-007-1	R6; R6.4	Lower	
			SERC201000620	CIP-007-1	R8; R8.4	Medium	
			SERC2012010717	CIP-004-3	R2; R2.3	Lower	
			SERC2012010718	CIP-004-3	R4	Lower	
			SERC2012010953	CIP-006-3c	R5	Medium	
			SERC2012010954	CIP-006-2	R2; R2.1	Medium	

			SERC2012010998	CIP-006-3c	R4	Medium	
			SERC2012011007	CIP-006-3c	R4	Medium	
			SERC2012011008	CIP-006-1	R1; R1.1	Medium	
			SERC2012011117	CIP-002-3	R3	High	
			SERC2012011161	CIP-002-3	R3	High	
			SERC2012011433	CIP-006-1	R3	Medium	
			SERC2012011434	CIP-005-1	R1; R1.1	Medium	
			SERC2012011435	CIP-007-1	R4; R4.2	Medium	
			SERC2012011437	CIP-007-1	R7; R7.3	Lower	
			SERC2013011699	CIP-006-3c	R1; R1.6.	Medium	
			SERC2013011706	CIP-006-3c	R1; R1.6.	Medium	
			SERC2013012206	CIP-006-3c	R4	Medium	
			SERC2013012431	CIP-004-3a	R4; R4.1	Lower	
			SERC2013012710	CIP-006-3c	R1; R1.6	Medium	
			SERC2013012712	CIP-004-1	R3	Medium	

CIP-002-1 R3 (SERC200900394)

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical

Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> R3.2. The Cyber Asset uses a routable protocol within a control center; or,
>
> R3.3. The Cyber Asset is dial-up accessible.

CIP-002-1 R3 has a "High" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL). During a Spot Check, SERC discovered that URE failed to identify all associated Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset.

During the Spot Check, SERC reviewed URE's CCA list and found that it did not include any network devices. URE had a number of network devices within its Electronic Security Perimeters (ESPs) at this time. These network devices were listed on URE's list of non-critical Cyber Assets, and all the network devices resided within an established ESP and Physical Security Perimeter (PSP). These network devices were Internet Protocol (IP) capable, connected to the URE network, and connected to the Cyber Assets that were identified on URE's CCA list. SERC determined that the network devices should have been identified as CCAs and included on the CCA list. SERC determined that URE omitted the network devices from its CCA list because of an internal URE misunderstanding.

Of the original identified network devices, URE added several switches and routers to its CCA list, left several switches and one router device on its non-critical Cyber Asset list, and retired or eliminated

several devices. None of the identified network devices were electronic access control and monitoring (EACM) devices.

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

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

SERC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, URE's failure to include the essential network devices on the CCA list could have left these devices without the protections that are afforded CCAs. However, the affected network devices resided within the secured ESP and PSP, thereby limiting and controlling access to the devices. URE did not detect or discover any actual security issues through the intrusion detection system (IDS) for any devices within the ESP during the time of the violation.

CIP-004-1 R4 (SERC200900399)

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

CIP-004-1 R4 provides in pertinent part:

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

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

During the Spot Check, URE failed to provide evidence that it maintained lists of personnel with authorized cyber access or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

Prior to the date of mandatory compliance, URE had identified several Cyber Assets used to support a certain application as CCAs and added them to URE's CCA list.

However, URE did not maintain lists of the individuals outside of URE with authorized cyber access to the application-associated Cyber Assets, which URE had identified as CCAs. Without a list of the individuals outside of URE with authorized cyber access to the application-associated Cyber Assets, URE could not ensure that those individuals were participating in the cyber security awareness program, were receiving cyber security training, or had valid personnel risk assessments (PRAs).

However, the application was isolated by design in its own demilitarized zone (DMZ) and was several security zones removed from any other CCA system behind a layered security model. This design prevented access to any other CCA through the application and would not allow the connecting party to view or manipulate any critical data pertinent to other CCAs, Critical Assets, the EMS, or URE's operation or control of the BPS.

URE eventually determined that the application-related Cyber Assets should not have been considered CCAs and should be removed from the CCA list.

SERC determined that URE had a violation of CIP-004-1 R4 for failing to maintain lists of personnel with authorized cyber access or authorized unescorted physical access to the application-related CCAs, including their specific electronic and physical access rights.

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 minimal and not serious or substantial risk to the reliability of the BPS. The application servers were protected within an ESP and PSP and were afforded the protections of CCAs. Individuals outside the ESP had read-only access to the application servers; outside users could not access any other CCAs within the ESP because the application servers were isolated in their own DMZ. Furthermore, URE classified the application-related devices as CCAs in error. The devices were not essential to the operation of Critical Assets and should not have been included on the CCA list.

CIP-009-1 R1 (SERC200900402)

The purpose statement of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices."

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
>
> R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
>
> R1.2. Define the roles and responsibilities of responders.

CIP-009-1 R1 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, SERC discovered that URE had a practice of shredding outdated business continuity plan (BCP) copies, and therefore was not able to provide evidence that recovery plans for CCAs were in place as of the date of mandatory compliance. URE provided a version of its BCP that defined roles and responsibilities of responders, but failed to specify required action in response to events of varying duration and severity. SERC also determined that the BCP failed to address the recovery of CCAs and instead focused on system level site recovery.

SERC determined that URE had a violation of CIP-009-1 R1 for failing to provide evidence that recovery plans for CCAs existed by the date of mandatory compliance.

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 lack of a detailed recovery plan could have delayed a quick and thorough recovery from a CCA failure. However, URE had a BCP in place which provided high-level recovery plans for a disaster scenario.

CIP-007-1 R7 (SERC201000573)

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

CIP-007-1 R7 provides:

> R7. Disposal or Redeployment — The Responsible Entity shall establish 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.
>
> 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-007-1 R7 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it did not have procedures for disposing of or redeploying some Cyber Assets within the ESP, specifically network equipment.

URE's disposal and redeployment procedures failed to address the disposal or redeployment of the network Cyber Assets identified during the Spot Check (NERC Violation ID SERC200900394). The network Cyber Assets were jointly maintained by two URE groups. Both groups erroneously believed that the other group was responsible for establishing and implementing the necessary disposal and redeployment procedures for these network Cyber Assets. As a result, URE was unable to demonstrate that it properly disposed of or redeployed network Cyber Assets during the time of the violation.

SERC determined that URE had a violation of CIP-007-1 R7 for failing to establish formal methods, processes, and procedures for disposal or redeployment of some Cyber Assets within the ESP, specifically network equipment.

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 have disposal and redeployment procedures

for all Cyber Assets within the ESP could have led to the removal or redeployment of devices containing CCA data and information without the proper measures having been taken to prevent the unauthorized retrieval of that data and information. However, URE had IDS in place and operational, and the IDS detected no issues regarding the network Cyber Assets. In addition, URE deployed multiple layers of security controls. These security controls included firewalls that prevented port scans from within or outside the ESP, two-factor authentication for all remote access into any ESP, a 30-minute lockout after three failed log-in attempts for all administrator user IDs, and logging for all Cyber Assets within the ESP (as technically feasible). Furthermore, URE provided some protections to the network Cyber Assets, including changing the passwords on the network Cyber Assets as required under CIP-007 R5.3.3 and including the network Cyber Assets in its annual Cyber Vulnerability Assessment (CVA).

CIP-007-1 R1 (SERC201000575)

CIP-007-1 R1 provides:

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

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

URE submitted a Self-Report to SERC stating that it had determined that changes to certain Cyber Assets within the established ESP, specifically network devices, were not evaluated for significance and tested to ensure that those changes did not adversely affect existing cyber security controls.

URE's test procedures for new Cyber Assets or significant changes to existing Cyber Assets failed to address the testing of the network Cyber Assets identified in the Spot Check (NERC Violation ID SERC200900394). The network Cyber Assets were jointly maintained by two URE groups. Both groups erroneously believed that the other group was responsible for establishing and implementing the necessary test procedures for these network Cyber Assets. As a result, URE was unable to quantify the number of significant changes involving network Cyber Assets that occurred or provide evidence that new network Cyber Assets or significant changes to those network Cyber Assets did not adversely affect existing cyber security controls.

SERC determined that URE had a violation of CIP-007-1 R1 for failing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls.

SERC determined the duration of the violation to be from 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 ensure that all significant changes to network Cyber Assets were tested for impacts to existing security controls could have reintroduced default accounts and passwords or created other vulnerabilities that could have been exploited. However, URE had IDS in place and operational, and the IDS detected no issues regarding the network Cyber Assets. In addition, URE deployed multiple layers of security controls. These security controls included firewalls that prevented port scans from within or outside the ESP, two-factor authentication for all remote access into any ESP, a 30-minute lockout after three failed log-in attempts for all administrator user IDs, and logging for all Cyber Assets within the ESP (as technically feasible). Furthermore, URE provided some protections to the network Cyber Assets, including changing the passwords on the network Cyber Assets as required under CIP-007 R5.3.3 and including the network Cyber Assets in its annual CVA.

CIP-007-1 R3 (SERC201000576)

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable

cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

URE submitted a Self-Report to SERC stating that it had not tracked, evaluated, or tested security-related patches for all Cyber Assets within the ESP, specifically for network equipment.

URE's security patch management program failed to address the tracking, evaluation of, testing, and installation of applicable cyber security software patches for the network Cyber Assets identified in the Spot Check (NERC Violation ID SERC200900394). The network Cyber Assets were jointly maintained by two URE groups. Both groups erroneously believed that the other group was responsible for establishing and implementing the necessary security patch management procedures for these network Cyber Assets. As a result, URE was unable to quantify the number of security patches for network Cyber Assets that it failed to assess within 30 days of the availability of the security patches.

SERC determined that URE had a violation of CIP-007-1 R3 for failing to track, evaluate, or test security-related patches for Cyber Assets, specifically network equipment, within the ESP.

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 track, evaluate, or test security-related patches for network Cyber Assets within the ESP could have left those network Cyber Assets vulnerable to exploit through recently-discovered vulnerabilities or other security-related deficiencies. However, URE had IDS in place and operational, and the IDS detected no issues regarding the network Cyber Assets. In addition, URE deployed multiple layers of security controls. These security controls included firewalls that prevented port scans from within or outside the ESP, two-factor authentication for all

remote access into any ESP, a 30-minute lockout after three failed log-in attempts for all administrator user IDs, and logging for all Cyber Assets within the ESP (as technically feasible). Furthermore, URE provided some protections to the network Cyber Assets, including changing the passwords on the network Cyber Assets as required under CIP-007 R5.3.3 and including the network Cyber Assets in its annual CVA.

CIP-004-1 R3 (SERC200900599)

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

CIP-004-1 R3 provides in pertinent part:

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

CIP-004-1 R3 has a "Lower" VRF and a VSL of Moderate.

During the Spot Check, SERC discovered that URE failed to conduct a PRA within 30 days of granting a contractor access to CCAs. Specifically, SERC discovered that URE granted a contractor authorized unescorted physical access to CCAs. Over two months later, URE revoked the contractor's access because it was no longer required. The contractor did not have a valid PRA during the time he had access to CCAs. URE did not realize that the contractor had access for more than 30 days without a valid PRA because an URE employee incorrectly documented the contractor's PRA approval date.

After the Spot Check concluded, URE reviewed all PRAs for all individuals with access to CCAs and found no other instances where it failed to conduct the required PRA within 30 days of granting access to CCAs.

SERC determined that URE had a violation of CIP-004-1 R3 for failing to conduct a PRA within 30 days of granting a contractor authorized unescorted physical access to CCAs.

SERC determined the duration of the violation to be from 31 days after URE granted the contractor access to CCAs, through when URE revoked the contractor's access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation involved less than one percent of individuals with CCA access. The contractor had access to CCAs for approximately two months before URE removed that access; access was removed because it was no longer required. The contractor had completed the required annual cyber security training, and the contractor passed a criminal background check several years prior. URE considered the contractor to be in good standing prior to, during, and after this violation.

CIP-002-1 R3 (SERC201000609)

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

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> R3.2. The Cyber Asset uses a routable protocol within a control center; or,
>
> R3.3. The Cyber Asset is dial-up accessible.

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

During a Spot Check, SERC discovered that URE failed to update its list of CCAs as necessary in two instances.

During the Spot Check, SERC selected a sample of CCAs to review. URE informed SERC that several of the sampled CCAs had been retired and were no longer used, but they were still present on the CCA list. SERC learned that the CCAs discovered during the Spot Check were associated with the EMS and were removed from service prior to the mandatory compliance date. URE removed these devices from its CCA list several years later.

In addition, SERC discovered that a group of systems, specifically EACM devices, had been placed onto the CCA list. URE eliminated remote access capabilities to its substations, making the EACM devices not essential to the operation of the Critical Assets. This occurred at some point before the mandatory compliance date, but these EACM devices remained on the CCA list until at least a year later.

SERC determined that URE had a violation of CIP-002-1 R3 because URE failed to update its list of CCAs as necessary in two instances.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE removed the CCAs identified during the Spot Check from its CCA list.

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 update its CCA list as required could have resulted in confusion because URE's documentation and physical site configuration would not have matched. Such a situation could have delayed URE's response to a cyber security incident or the restoration of CCAs using the URE recovery plan. URE's failure to remove the retired EMS devices from its CCA list demonstrates a lack of attention to detail and indicates a flawed review process. However, the devices involved in this violation were on the CCA list in error and were not essential to the operation of any Critical Assets.

CIP-005-1 R2.2 (SERC201000611)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-1 R2 provides in pertinent part:

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).

***

R2.2. 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.

***

CIP-005-1 R2.2 has a "Medium" VRF and a "Severe" VSL. During the Spot Check, URE failed to provide evidence that explicit access permissions were used as part of its access control model such that only ports and services necessary for operations or monitoring were enabled.

SERC discovered that URE used an older legacy EMS. This model required the ability to route between internal firewalls in order to permit proper communication between the separate ESPs that make up the URE control network. The EMS control network allowed traffic to communicate internally and denied traffic that was not a part of the internal network. In order to function without creating operational impacts, the EMS control network firewall rule sets allowed a wide range of IP addresses. Additionally, the legacy EMS system required a wide range of ports and services, used at random, due to the asynchronous routing. Traffic that flowed through one firewall for ingress may have a different firewall identifier for its egress traffic. Due to the complexity of the legacy EMS, the EMS vendor informed URE that the wide ranges within the firewall rule bases were required for the system to operate properly.

For any necessary external connectivity, the URE security model passed traffic from the EMS control network to an intermediary DMZ where a data broker assumed control of the data and sent it outside of the EMS network. This traffic was tightly controlled and logged by external facing firewalls which were configured to deny access by default.

SERC reviewed the network diagrams and firewall rules associated with the internal EMS control network firewalls and the external facing firewalls that segment the control network from the larger corporate network. SERC confirmed that for the internal firewalls, URE had firewall rules that denied

access by default to external traffic from the corporate network on the internet, and permitted access between the internal firewalls, to allow the routing used by the EMS control network. URE was unable to specifically document the ports and services that needed to be enabled because ports opened and closed based on the EMS requirements and the routing being utilized.

For the external facing firewalls between the controls network and the corporate network, SERC confirmed that the firewall rules denied access by default for traffic passing through the firewalls. All communication paths, both internal to the EMS as well as external to the DMZ, were owned and maintained by URE. URE also utilized an IDS that provided additional security to the EMS.

URE attested that it attempted to restrict and limit the ports and services within the EMS control network after the Spot Check, but encountered operational impacts due to the system requirements of the legacy EMS. Although URE was able to disable some unneeded ports, it was limited in the actions it could take without creating issues on its EMS network.

SERC determined that URE was in violation of CIP-005-1 R2.2 for failing to use explicit access permissions as part of its access control model such that only ports and services necessary for operations or for monitoring Cyber Assets within the ESP were enabled.

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

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to disable the ports and services which were not required for normal or emergency operations could have permitted available ports to become potential attack vectors into the ESP. If an attacker breached the external facing firewalls, the attacker could have gained access to all of URE's ESPs and the CCAs within those ESPs. Such an attack could have disrupted URE's operation of and control over its entire portion of the BPS. URE's external facing firewalls were configured securely with a deny-access-by-default rule. In addition, URE had a fully operational IDS to alert URE personnel of any intrusions. Vendor documentation supported the open firewall rules on the EMS control network in order to keep the EMS functional and not impose risk to the BPS.

CIP-005-1 R4.5 (SERC201000612)

CIP-005-1 R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security

Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

***

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

***

CIP-005-1 R4.5 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, URE was able to retrieve only a small part of a CVA to show to the SERC auditors as evidence of compliance with CIP-005-1 R4.5. URE claimed that it conducted the required CVA, meeting all actions specified as well as producing a results document and action plan for all identified vulnerabilities. However, URE claimed that the documentation could not be recovered because it was saved on a file server that crashed, and this file server was not being backed up. At the time, the CVA results and action plan were a single document, and this document was not archived. The small portion of the CVA that URE was able to produce did not show specific activities related to its assessment of the ESP access points.

SERC determined that URE had a CVA process in place, and that URE conducted some of the CVA activities required by the Standard in that particular year.

During the Spot Check, URE presented the CVA results from the following year. SERC did not identify any problems with this CVA.

SERC determined that URE had a violation of CIP-005-1 R4.5 for failing to maintain documentation of the results of the CVA of the access points to the ESPs, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

SERC determined the duration of the violation to be from the first day after the year in which the CVA was required to be performed through when URE completed the following year's CVA.

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 maintain documentation of the results of its CVA of the access points to the ESP could have left any identified vulnerabilities unresolved until URE conducted the next year's CVA. However, URE had multiple layers of security, including fully staffed

security and operational personnel that monitored the system for actual cyber vulnerabilities or intrusions. URE had IDS in place to help protect from attacks from inside and outside the ESP. Antivirus and malware prevention software was enabled on Cyber Assets, as technically feasible, to protect from both internal and external threats. Furthermore, URE conducted its CVA of the access points to the ESP within the following year. The following year's CVA covered all systems in service and resulted in only three significant findings, which were documented and addressed in action plans.

CIP-005-1 R5.2 (SERC201000613)

CIP-005-1 R5 provides in pertinent part:

> 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.
>
> ***
>
> 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.
>
> ***

CIP-005-1 R5.2 has a "Lower" VRF and a "Severe" VSL.

During the Spot Check, SERC discovered that URE failed to maintain documentation of all interconnected Cyber Assets within the ESP. Specifically, URE had ESP documentation and changed the Cyber Assets within the ESP, but failed to update its ESP documentation within 90 days of its modification of the network. The SERC spot check team found one instance where URE added Cyber Assets within an ESP via an authorized change request, but failed to add the new Cyber Assets to the ESP documentation until approximately seven months later. Additionally, during the physical site reviews, URE was unable to reconcile its ESP documentation with the physical inventory of Cyber Assets in service at the sites. URE had removed four Cyber Assets from the network but failed to update its ESP documentation within 90 days. In total, five Cyber Assets were affected.

SERC determined that URE had a violation of CIP-005-1 R5.2 for failing to update its ESP documentation within 90 days of its modification of the network.

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 update its ESP documentation within 90 days could have left those affected Cyber Assets without proper security measures, led to unauthorized changes or modifications to Cyber Assets within the ESPs, or delayed recovery of CCAs. However, URE's EACM devices did not detect any conditions that required investigation of the involved ESPs during the violation. Furthermore, this violation involved a total of five Cyber Assets.

CIP-006-1 R1.8 (SERC201000614)

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

CIP-006-1 R1 provides in pertinent part:

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

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

During the Spot Check, SERC discovered that URE failed to afford Cyber Assets used in the access control and monitoring of the PSPs the protective measures specified in CIP-006-1 R1.8.

SERC determined that URE failed to afford the protective measures required by CIP-007 R5.3.3 and CIP-007 R7.3 to all physical access control system (PACS) devices. The SERC spot check team sampled a number of PACS devices and found that the sampled devices failed to comply with CIP-007 R5.3.3 in at least three instances and with CIP-007-2 R7.3 in at least two.

The first issue in which URE failed to provide its PACS devices the protective measures specified in CIP-007 R5.3.3 involved several PACS servers with default administrative accounts that could not be

deleted. In order to secure these accounts, URE used a password vault. The password vault allowed for the application of encrypted passwords to the default administrative accounts. No more than several corporate administrators had access to the password vault. In order to access the password vault, URE required users to use their own individually-assigned accounts, which were subject to active directory rules that required passwords to be changed every 45 days and enabled the tracking of all user activity. This arrangement prevented multiple users from knowing the passwords to the default administrative accounts, but left the default administrative accounts available and usable as needed in an emergency situation. As a result of this arrangement, URE did not change the default administrator passwords on an annual basis for any of the PACS servers.

The second issue in which URE failed to provide its PACS devices the protective measures specified in CIP-007-1 R7.3 involved work orders associated with the disposal or redeployment of PACS Cyber Assets. URE had procedures in place to erase or destroy sensitive cyber security data from PACS Cyber Assets that would be disposed of or redeployed. These procedures called for the creation of work order tickets that would serve as documentation to record the actions taken to erase or destroy sensitive cyber security data. SERC reviewed the work orders associated with three PACS device disposals it discovered during the Spot Check and determined that the work orders lacked clear details required by URE's procedures to ensure that URE had properly erased several PACS servers and one PACS control panel before returning them to the vendor.

SERC determined that URE had a violation of CIP-006-1 R1.8 because it failed to afford the protective measures required by CIP-007 R5.3.3 and CIP-007 R7.3 to all PACS devices.

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 minimal and not serious or substantial risk to the reliability of the BPS. The default administrator passwords for the PACS servers were stored on an encrypted password vault and could only be accessed by several administrators, who had to use their individual user account credentials to log-in to the password vault and Cyber Assets. URE's active directory policy forced the administrators to change their individual account passwords at least every 45 days. In addition, the default administrator account password met the complexity requirements of CIP-007-1 R5.3.1 and R5.3.2.

With respect to the CIP-007 R7.3 issue, although the work order tickets associated with the disposal or redeployment of three PACS Cyber Assets lacked the detail required by its documented procedures,

URE had additional work order tickets that showed the procedures were generally being followed by users.

CIP-006-1 R6 (SERC201000615)

CIP-006-1 R6 provides:

> R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:
>
> R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
>
> R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.
>
> R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

CIP-006-1 R6 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, SERC discovered that URE's testing program failed to ensure that all physical security systems under CIP-006-1 R2, R3, and R4 functioned properly.

URE had a documented physical security plan that required URE to test the physical security systems at each site at a minimum of once every three years and required the retention of all records specified in CIP-006-1 R6.2 and R6.3. Operationally, URE performed the site testing annually to ensure the integrity of the security systems and to identify more quickly any potential physical security issues. During the Spot Check, a SERC auditor exited "egress-only" doors at two PSPs and was then able to re-enter the PSPs via the motion detector request-to-exit (REX) device above the doors.

In the first instance, the auditor exited the egress-only door at a PSP and was able to regain access via the same door after slipping paper under the door in an effort to activate the REX device. URE staff present believed that the REX device was positioned to activate the lock release too close to the door, allowing the paper to trigger the latch release. URE's physical security staff immediately repositioned the REX device to detect personnel as they approached the door instead of when they were at the door. URE never considered the possibility that the REX could be activated from outside the PSP.

In the second instance, the auditor exited an egress-only door at a PSP allowed the door to close behind him. The auditor then immediately attempted to activate the REX device for re-entry by sliding a piece of paper between the door jam and the door, and was able to pull open the door. SERC reviewed the data provided by URE, including the log of the forced entry alarm received by the security console for this specific incident and the security photos captured. In reviewing the logs provided, SERC concluded that the alarm micro re-engaged as soon as the door closed, but the electronic strike lock did not engage immediately when the door closed. URE confirmed that this was a design configuration. The electronic lock took 10 seconds to re-engage, while the door alarm contacts re-engaged upon contact. The SERC auditor was able to gain re-entry due to this lag in the electronic lock, not the attempt to trigger the REX device from outside the PSP. URE's physical security staff immediately repositioned the REX device to detect personnel as they approached the door instead of when they were at the door.

SERC determined that URE had a violation of CIP-006-1 R6 for failing to implement a maintenance and testing program that would ensure that all physical security systems under R2, R3, and R4 functioned properly.

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 minimal and not serious or substantial risk to the reliability of the BPS. The 10-second delay between closure of the door to the PSP and re-engagement of the electronic lock could have provided an intruder a limited opportunity to gain access after an authorized person exited. However, the authorized person exiting the PSP likely would have noticed any intruders. In addition, the security monitoring system would have issued a forced entry alarm as soon as the door was opened by an intruder because the door contacts re-engaged upon the door's closure. URE personnel would have responded immediately to any forced entry alarm. Furthermore, security cameras were installed at the affected access points, and those cameras were monitored by security personnel at all times.

CIP-007-1 R1 (SERC201000616)

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

CIP-007-1 R1 provides:

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

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

During the Spot Check, SERC discovered that URE failed to document test results for significant changes to Cyber Assets within the ESP. The SERC spot check team reviewed changes (pursuant to CIP-003-2 R6) and the associated CIP-007-2 R1 test procedure results for sampled Cyber Assets. The SERC spot check team discovered that, for at least three changes which fell under the "significant change" language of CIP-007-2 R1, URE could not provide evidence for the performance or documentation of the security testing. In addition, the SERC spot check team found that, for other sampled Cyber Assets which were tested, URE conducted the security testing after the upgrades were installed on the production devices.

URE had a policy document on change management that provided guidance on how and when testing of significant changes should occur, which also addressed routine and emergency changes. URE also maintained an evaluation criteria procedure document, which listed a series of check box questions used to determine which changes to the systems would be considered ”significant.” The questions pertained to the various systems in service based on the infrastructure or work practices, or the application being modified, replaced, or added.

Due to the complexity of the system reviews required by its evaluation criteria procedure document, URE personnel inconsistently applied the significant change evaluation and security controls testing

questions. SERC determined that these human performance inconsistencies led to the missed and delayed testing that was identified in the Spot Check.

SERC determined that URE had a violation of CIP-007-1 R1 for failing to document test results for significant changes to Cyber Assets within the ESP.

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 test changes prior to implementation on a production environment could have compromised the functionality of CCAs that reside on the production system. Additionally, URE's failure to test all significant changes, including to third-party software and firmware, increased the probability that vulnerabilities could be introduced. However, URE had IDS in place and operational, and the IDS did not detect or log any issues associated with the untested changes to the affected Cyber Assets. The affected Cyber Assets resided within the secured ESP and PSP, thereby limiting access. In addition, URE required two-factor authentication for all remote access into any ESP and imposed a 30-minute lock-out after three failed log-in attempts for all administrator user IDs. URE also had logging enabled for all Cyber Assets within the ESP, as technically feasible. URE experienced no problems with the affected Cyber Assets after the significant changes.

CIP-007-1 R2 (SERC201000617)

CIP-007-1 R2 provides:

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

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

During the Spot Check, SERC discovered that URE failed to ensure that only those ports and services required for normal and emergency operations were enabled.

The SERC spot check team sampled a number of CCAs as well as non-critical Cyber Assets within the ESPs. The SERC spot check team found numerous devices that had ports enabled which URE had not designated to be enabled in the baseline/port standard document it had developed. URE was unable to provide documentation demonstrating the need for these ports to remain enabled on the sampled devices. Further, URE did not request Technical Feasibility Exceptions (TFEs) for these devices under R2.3.

URE had an older EMS in service at the time of the Spot Check. This legacy EMS presented unique challenges to the identification of which ports and services were required for normal and emergency operations. Scanning for ports and services could have caused unforeseen operational impacts by negatively affecting the legacy EMS and subsequently impacting the BPS. Thus, URE believed it could not use automated tools to examine ports and services to account for all production operational states.

The legacy EMS also did not have a fully functional test model. As a result, URE could not test the removal of ports and services to identify which ones were required for normal and emergency operations. Such an effort could have negatively impacted the EMS and potentially the BPS. While URE did not have TFEs for the older Cyber Assets associated with the legacy EMS, it had approved TFEs for the older network devices used in the communication pathways. URE did not request TFEs for the older Cyber Assets within the ESP because it believed it could demonstrate an operational need for all ports and services that were open and available. In an effort to manage ports and services under its given constraints, URE used a blacklisting approach for Cyber Assets within the ESP. The blacklisting approach required that each specific port and service not needed for normal and emergency operations be listed for denial on each Cyber Asset. However, URE was unable to demonstrate that only ports and services required for normal and emergency operations were enabled. URE acknowledged that it should have explored and implemented a whitelisting approach (i.e., listing the ports and services that are authorized) to deal with the challenges posed by the legacy EMS.

SERC determined that URE had a violation of CIP-007-1 R2 for failing to ensure that only those ports and services required for normal and emergency operations were enabled on a number of CCAs and non-critical Cyber Assets within the ESPs.

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 disable open ports and services that were not needed for normal or emergency operation on Cyber Assets within the ESP could have allowed attackers to attack or otherwise exploit vulnerabilities in the Cyber Assets, including the EMS. Such an attack could have disrupted URE's operation of and control over its entire portion of the BPS. However, all Cyber Assets resided within the secured ESP and PSP, so access was limited and controlled. URE had IDS in place and operational. URE deployed multiple layers of security controls. These security controls included outward-facing firewalls that used a deny-by-default model, firewalls that prevented pings and port scans, two-factor authentication for all remote access into any ESP, and the imposition of a 30-minute lock-out after three failed log-in attempts for all administrator user IDs. Finally, URE had logging enabled for all Cyber Assets within the ESP, as technically feasible.

CIP-007-1 R5.3.3 (SERC201000618)

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> ***
>
> R5.3. 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 5.3.3 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, SERC discovered that URE failed to demonstrate that it changed passwords at least annually for sampled Cyber Assets within the ESP. The SERC spot check team found that, for at least one of the sampled Cyber Assets within the ESP, URE had not changed at least one of the account passwords on an annual basis.

In total, URE had user passwords on several Cyber Assets within the ESP, including one CCA and several non-critical Cyber Assets, which were not changed annually. Individual users failed to follow URE's established user account and password policies and instead relied on the fact that users had to utilize a two-factor login in order to gain access to Cyber Assets within the ESP. At the time of the violation, URE did not have the technical means to require users to change their passwords annually. URE determined that some users erroneously believed that because two-factor login was used for all Cyber Asset log-ins, changing the user passwords on the Cyber Assets was not required.

SERC determined that URE had a violation of CIP-007-1 R5 for failing to change passwords at least annually for sampled Cyber Assets within the ESP.

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 change the passwords at least annually increased the risk that malicious actors could have discovered and exploited the unchanged passwords. However, the passwords used on the affected Cyber Assets met the complexity requirements of the CIP Standards, as technically feasible, and internal URE policies. Logging on to the affected Cyber Assets required two-factor authentication using a token code that changed every 60 seconds. In addition, all affected Cyber Assets were secured within an ESP and PSP.

CIP-007-1 R6.4 (SERC201000619)

CIP-007-1 R6 provides in pertinent part:

> 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.

***

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

***

CIP-007-1 R6.4 has a "Lower" VRF and a "Severe" VSL.

During the Spot Check, URE failed to provide evidence that it retained cyber security logs for 90 days for a sampled device within the ESP. The SERC spot check team requested sample security logs from Cyber Assets within the ESP. URE could not provide evidence of the retention of logs for at least 90 days for at least one of the sampled Cyber Assets within the ESP. The device in question was specialized and did not have any remote logging capabilities. URE had not sought a TFE for that particular device.

URE determined that the violation was not caused by the logging being done by the Cyber Assets. Instead, it was caused by a failure of the centralized log server that received the logs from other Cyber Assets for aggregation and retention. The large volume of logs generated and monitored from across the URE network overwhelmed the centralized log server during periods of high logging activity, which resulted in some logs not being received and archived. Since this failure occurred only during high logging activity, URE was unable to quantify the amount of logs that were not received and maintained for the required 90 days. SERC was therefore unable to determine the number of CCAs and non-critical Cyber Assets within the ESP that were involved in this violation. This violation affected only the Cyber Assets within the ESP and did not affect the logging and monitoring of access points, specifically firewall logs.

SERC determined that URE had a violation of CIP-007-1 R6.4 for failing to retain all logs specified in CIP-007-1 R6 for ninety calendar days for a sampled device within the ESP.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE's failure to retain logs related to security events for 90 calendar days could have led to the loss of important security information required for a thorough investigation. However, all Cyber Assets resided within the secured ESP and PSP. URE had IDS in place and operational. In addition, URE deployed multiple layers of security controls. These cyber security controls included properly-configured outward facing firewalls that used deny-by-default rules and technical controls that prevented port scans from inside or outside of the ESP. Also, URE required two-

factor authentication for all remote access into any ESP and imposed a 30-minute lock-out after three failed access attempts for all administrator user IDs.

CIP-007-1 R8.4 (SERC201000620)

CIP-007-1 R8 provides in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R8.4. Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-007-1 R8.4 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, URE failed to provide evidence that it conducted a CVA of all Cyber Assets within an ESP for one particular year. The SERC spot check team asked URE to provide evidence that it conducted the CVA for that year. Due to a change in its assessment tools, URE was only able to retrieve a small part of the CVA for that year to show as evidence. While URE did provide evidence of the assessment of a single Cyber Asset within the ESP, it did not provide any other evidence to demonstrate that all Cyber Assets within all ESPs had been assessed for the that year.

URE claimed that it conducted the required CVA for that year, meeting all actions specified as well as producing a results document and action plan for all identified vulnerabilities. URE could not provide full documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan. URE claimed that the full results of the CVA for that year were saved on a file server that crashed; the file server was not being backed up and the contents could not be recovered. At the time, the CVA results and action plan were a single document, and this document was not archived.

URE was able to provide documentation showing that it had a cyber vulnerability assessment process, as required by CIP-007-1 R8.1, and that it had conducted some of the activities required by CIP-007-1 R8.2 and R8.3.

During the Spot Check, URE presented its CVA results for the subsequent year. The SERC audit team found no problems with the subsequent year's CVA.

SERC determined that URE had a violation of CIP-007-1 R8.4 for failing to maintain documentation of the results of the CVA, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

SERC determined the duration of the violation to be from the first day after the year the CVA was to be performed, through when URE completed the subsequent year's CVA.

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 maintain documentation of the results of its CVA of the Cyber Assets within the ESP could have left any identified vulnerability unresolved until URE conducted the next year's CVA. However, URE deployed multiple layers of security, including fully staffing its security and operational personnel to monitor the system for any actual cyber vulnerabilities or intrusions. URE had IDS in place and operational to help protect from attacks from inside and outside the ESP. Antivirus and malware prevention software was enabled on Cyber Assets, as technically feasible, to protect from both internal and external threats. Furthermore, URE conducted its subsequent year CVA of all Cyber Assets within the ESP on within seven months of the previous year's CVA being due. The subsequent year CVA covered all systems in service and resulted in three significant findings.

CIP-004-3 R2.3 (SERC2012010717)

The purpose statement of Reliability Standard CIP-004-3 provides: "Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-3 R2 provides:

> R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior

to their being granted such access except in specified circumstances such as an emergency.

R2.2. Training shall cover the policies, access controls, and procedures as developed for the Critical Cyber Assets covered by CIP-004-3, and include, at a minimum, the following required items appropriate to personnel roles and responsibilities:

R2.2.1. The proper use of Critical Cyber Assets;

R2.2.2. Physical and electronic access controls to Critical Cyber Assets;

R2.2.3. The proper handling of Critical Cyber Asset information; and,

R2.2.4. Action plans and procedures to recover or re-establish Critical Cyber Assets and access thereto following a Cyber Security Incident.

R2.3. The Responsible Entity shall maintain documentation that training is conducted at least annually, including the date the training was completed and attendance records.

CIP-004-3 R2.3 has a "Lower" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that it failed to complete the annual cyber security training in one year for one contract employee with authorized physical access to CCAs.

The contract employee was trained on one date and was granted CIP access approximately seven months later. . At the time, URE's procedure required training every twelve months. The procedure was revised to require training within the calendar year, but no later than 15 months. Due to an oversight, the contract employee did not receive the subsequent year's training until seven days past the 15-month training requirement. This oversight affected less than one percent of employees and contractors with authorized access to CCAs.

SERC determined that URE had a violation of CIP-004-3 R2.3 for failing to complete annual cyber security training for one contract employee with authorized physical access to CCAs.

SERC determined the duration of the violation to be from the date by which the contractor should have received the annual cyber security training through the date when the contractor received the annual cyber security training.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Less than one percent of employees and contractors with permitted access to CCAs missed the annual training requirement, and it was missed by seven days. Furthermore, the contract employee had a current PRA on file.

CIP-004-3 R4 (SERC2012010718)

CIP-004-3 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-004-3 R4 has a "Lower" VRF and a "Lower" VSL.

URE submitted a Self-Report to SERC stating that it had given unescorted physical access to CCAs to two contract employees without performing the appropriate background screenings and training. URE reported that it did not track these two contract employees on its CCA access lists.

While manually coding security badges with some non-CIP access permissions, URE mistakenly gave two contract employees physical access to CCAs by coding their badges with physical access rights. The two employees were not added to URE's CCA access list. The two employees did not require physical access to the CCAs, and they had not received cyber security training or had PRAs performed. Approximately one month later, URE removed the two contract employees' physical access rights after discovering the issue during a reconciliation of the previous physical access system with the current physical access system. According to URE, during the time that the two contract employees had

physical access, the badges were not used to access any PSPs. This issue involved less than one percent of employees with authorized access rights.

SERC determined that URE had a violation of CIP-004-3 R4 for granting physical access rights to two contract employees without tracking these individuals on its CCA access lists.

SERC determined the duration of the violation to be from the date URE gave the two contract employees physical access rights to CCAs, through the date when URE removed the access rights.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Neither contract employee knew his badge had been coded for physical access, neither attempted to access any PSPs, and both were in good standing with URE.

CIP-006-3c R5 (SERC2012010953)

The purpose statement of Reliability Standard CIP-006-3c provides in pertinent part: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets."

CIP-006-3c R5 provides:

> R5. Monitoring Physical Access —The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. 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 submitted a Self-Report to SERC stating that it had a lapse in the alarm system monitoring of physical access points to several PSPs for a period of approximately 10 hours.

On the day in question, a security guard failed to launch properly the alerting application used by URE at the start of the shift. Since the tool was improperly launched, it did not provide the data about PSP anomalies that required immediate review. This condition existed until about ten hours later.

SERC learned that there were six alarms during this time period. Each occurred at the same door at the control center PSP. The security guard working the next shift spoke to the person who triggered the alarms. The person was an authorized individual who set off the door alarms in error while performing regular job duties. According to URE, an investigation of the alarms triggered at the PSPs (conducted on the same day as the discovery of the violation) revealed that there were no security breaches or unauthorized access.

SERC determined that URE had a violation of CIP-006-3c R5 for failing to implement alarm system monitoring of the physical access points to several PSPs for a period of approximately 10 hours.

SERC determined the duration of the violation to be for approximately ten hours on the day in question.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to monitor PSPs for unauthorized access attempts could have allowed an unauthorized user to gain physical access, which greatly increased the risk of CCAs being compromised or rendered inoperable. However, there were no security breaches or unauthorized accesses for the duration of the violation. The individual that set off the alarms was authorized for access and set off the alarms in error while performing regular job duties.

CIP-006-2 R2.1 (SERC2012010954)

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

CIP-006-2 R2 provides in pertinent part:

> R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
>
> R2.1. Be protected from unauthorized physical access.

***

CIP-006-2 R2.1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to protect a security panel used to control access to CIP-protected perimeter doors against unauthorized physical access.

URE discovered that a panel, which was used to authorize access to PSP perimeter doors, did not have protection from unauthorized physical access for approximately four months. The panel at issue controlled physical access to a PSP that contained several PACS servers.

SERC determined that URE had internal procedures that required the placement of PACS devices within an established PSP. In this instance, however, there was a miscommunication regarding the type of assets to which the panel controlled access.

SERC determined that URE had a violation of CIP-006-2 R2.1 for failing to protect a panel which was used to control access to PSP perimeter doors from unauthorized physical access.

SERC determined the duration of the violation to be from the date when the panel was configured to allow physical access to a PSP through the date when the PSP doors were reallocated to a different panel that was protected from unauthorized physical access.

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 secure the security panel within a secured perimeter could have allowed access to Critical Assets and the associated CCAs, potentially impacting the BPS. However, the panel was secured within a restricted area that had controlled access.

CIP-006-3c R4 (SERC2012010998)

CIP-006-3c R4 provides:

> R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.

- Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
- Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-3c R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it failed to control access to physical keys used for PSPs after two employees were reassigned and no longer required physical access.

URE had a documented key control procedure (key procedure) that specified that the asset owner or designee role would be responsible for maintaining key inventory, key assignments, issuance records, and quarterly key audits. The key procedure also required the designated key holder to surrender their key within seven days of a transfer or within 24 hours in the case of termination to the asset owner or designee having responsibility for protected site key management.

URE discovered during an internal compliance review that it did not follow its key procedure in two instances. Two site supervisors transferred to new roles, but URE did not collect the keys assigned to them within seven days as required by its key procedure. In the first instance, the supervisor no longer needed access to CCAs, and URE removed the supervisor from the CCA access list on the same day. However, the supervisor retained the key for over 100 days. In the second instance, URE asked the supervisor to retain access to CCAs in order to support and provide back-up to the new supervisor. However, the second supervisor's key was not collected and was last known to be in the supervisor's possession (*i.e.*, locked and secured in the supervisor's desk) over a year prior to the date of the transfer. URE changed out the locksets affected by the lost key.

SERC determined that URE had a violation of CIP-006-3c R4 for failing to control access to physical keys used for PSP access after two employees were reassigned and no longer required physical access.

SERC determined the duration of the violation to be from the date when the lost key was last known to be secured through the date when the locksets were changed in response to the lost key.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Any use of physical keys would send an immediate alarm to the URE security console and result in an immediate response and investigation. URE determined that no alarms were triggered by use of the physical keys and confirmed that there had been no use of the physical key that corresponded to any received forced entry alarms. Forced entry alarms trigger video cameras to begin recording at the location of the forced entry alarm. The keys involved provided access to approximately 15% of Critical Assets. Lastly, the lost key was unmarked and unidentifiable as belonging to the entity or any Critical Asset, so a person finding the key would have no way of knowing to what it provided access.

CIP-006-3c R4 (SERC2012011007)

CIP-006-3c R4 provides in pertinent part:

> R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> ***

CIP-006-3c R4 has a "Medium" VRF and a "Severe" VSL. URE

URE submitted a Self-Report to SERC stating that a locking mechanism on a PSP door malfunctioned and did not properly latch, allowing a former employee without authorized access to enter.

On the day in question, a recently-retired employee who did not have authorized access permissions opened a PSP door at an URE facility and gained access without presenting a valid badge to the badge reader. Due to the former employee's retirement, the former employee's access permissions to the facility were revoked two days earlier, which was within the allowed timeframe. The former employee had been allowed to keep his badge with general building access and parking access permissions after retiring, but was not allowed to retain access to the PSP in question.

In this instance, the former employee did not realize that his access privileges were no longer valid and attempted to badge into the PSP door to visit an employee who worked within the secured PSP. The former employee was able to access the PSP due to a malfunction of the access door, which caused it to become stuck in the frame just short of the point that the lock mechanism would engage. All of the access door's alarm contacts were functional and properly engaged, and security personnel received a

forced entry alarm when the former employee opened the door without first presenting a valid access badge. Security personnel immediately responded to the forced entry alarm to investigate.

URE had a physical security plan that detailed how it should create secured PSPs and comply with CIP-006 R1 through R8. Additionally, URE had a physical access policy that provided guidance on how physical access controls should be managed. SERC found that these plans addressed all necessary requirements.

SERC determined that URE had a violation of CIP-006-3c R4 for failing to ensure the proper functioning of a locking mechanism on a PSP, which malfunctioned and allowed a former employee without authorized access to enter.

SERC determined the duration of the violation to be from the date when the former employee gained access to a PSP without proper authorization through the date when the broken door was repaired and returned to normal operations.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All of the access door's alarm contacts were functional, and security personnel received a forced entry alarm when the former employee opened the door. Security personnel responded immediately to investigate the forced entry alarm and implemented heightened security procedures for the PSP access point until the door was repaired. The PSP was manned at all times. Personnel within the PSP had the former employee in their line of sight while he was within the PSP, escorted the former employee while within the PSP, and ensured that the visitor log was properly filled out to account for the former employee. The former employee was in good standing with the company and had previously been screened, trained, and authorized to have unescorted physical access within the PSP. The former employee was within the PSP for five minutes and did not attempt to access any of the CCAs within the PSP during that time. Security personnel subsequently reviewed video footage and confirmed that there had been no other prior occurrences of unauthorized access.

CIP-006-1 R1.1 (SERC2012011008)

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

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> R1.1. 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 R1.1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it terminated a Technical Feasibility Exception (TFE) for an incomplete six-wall border at a PSP prior to completing its mitigation efforts.

URE intended to end the need for the TFE by installing wire mesh barriers at the relevant PSPs. URE terminated the TFE one year earlier than the initial proposed TFE termination date. URE did not complete the final actions to create a six-wall perimeter at one of the PSPs included under the TFE until over a month after URE terminated the TFE. SERC determined that the cause of this violation was a breakdown in the internal communications between the field crew responsible for securing the six-wall boundary and the administration staff responsible for filing and terminating the TFE.

During a Compliance Audit, SERC discovered that URE had openings in existing PSPs that were larger than 96 square inches in two instances. In the first instance, the SERC audit team discovered an opening located beneath the raised floor of a URE control center door. In the second instance, the SERC audit team discovered an opening located above the URE PSP false ceiling. Prior to SERC's discovery, the existence of these openings was unknown.

URE submitted a Self-Report to SERC stating it found 14 unidentified openings that exceeded 96 square inches in its existing PSPs. SERC determined that all 14 openings identified in the Self-Report existed since the date of mandatory compliance and that URE did not deploy or document alternative measures to control physical access under a filed TFE.

SERC determined that URE had a violation of CIP-006-1 R1.1 for failing to establish completely enclosed ("six-wall") borders at all PSPs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE established the six-wall borders at all PSPs.

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 failure of URE to secure properly 17 openings in its PSPs could have allowed unauthorized individuals physical access to CCAs; these CCAs could have been compromised or sabotaged, affecting the BPS. However, an individual attempting to exploit these unsecured openings would have required either a special tool to lift raised floor panels or a ladder or some other climbing aid to access. Access would have been impeded by obstacles such as ductwork, wiring conduit, or cable trays. Furthermore, the sites had closed-circuit camera monitoring in place. Lastly, the IDS and real-time monitoring and alerting of the Cyber Assets within the ESP remained intact throughout the duration of the violation.

CIP-002-3 R3 (SERC2012011117)

The purpose statement of Reliability Standard CIP-002-3 provides: "Standard CIP-002-3 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-002-3 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
>
> R3.2. The Cyber Asset uses a routable protocol within a control center; or,
>
> R3.3. The Cyber Asset is dial-up accessible.

CIP-002-3 R3 has a "High" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that it had established a remotely accessible IP connection to Cyber Assets within a Critical Asset, thereby creating CCAs, without establishing the proper ESPs and PSPs.

On the day in question, a technician working on a line relay inside an URE substation that was classified as a Critical Asset experienced problems with the relay calculations. In an effort to remedy the issue and get the line relay commissioned and in service, the technician connected the local and isolated substation network, which was intentionally isolated from other networks by design, to the corporate network in order to provide remote IP access for support purposes. The network connection was in place for approximately 30 minutes, by which point the technician had fixed the issue and disconnected the substation network from the corporate network.

SERC determined that URE created CCAs when it connected the substation's local network to the corporate network, which established a routable network with routable Cyber Assets essential to the Critical Asset substation. The CCA list did not account for these CCAs when URE established the IP connection between the two networks. The technician's actions also created a condition in which the newly created CCAs existed outside of a documented ESP and were not protected within a documented PSP.

SERC determined that URE had a change management process in place to ensure all changes to CCAs were managed to meet the requirements of the CIP Standards, but a URE technician failed to follow the change management process in this instance.

SERC determined that URE had a violation of CIP-002-3 R3 for creating CCAs without establishing the proper ESPs and PSPs to protect them.

SERC determined the duration of the violation to be from when the technician connected the local substation network to the corporate network through when the technician terminated the connection (approximately 30 minutes).

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 consider and protect the newly-created CCAs increased the risk that the CCAs could be compromised or rendered inoperable. Compromised CCAs could have been used to send inaccurate information to the EMS, which in turn could have caused the loss of monitoring and control of the BPS. However, the local substation network was connected to

the corporate network for approximately 30 minutes, and the on-site technician was at the Critical Asset site and working on the relay for the entire duration of the connection. Furthermore, in order to gain remote access to the local substation network, an individual would have required access rights to the corporate network, the IP address of the substation relay, knowledge of how to establish remote access to the substation relay and how to use the relay's software, and the substation relay's log-in information.

CIP-002-3 R3 (SERC2012011161)

CIP-002-3 R3 provides in pertinent part:

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

CIP-002-3 R3 has a "High" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that had established a remotely accessible IP connection to Cyber Assets within a Critical Asset, thereby creating CCAs, without establishing the proper ESPs and PSPs.

During routine construction activities at a URE substation classified as a Critical Asset, URE's technicians were having problems getting some protective devices to communicate with the substation's Remote Terminal Unit (RTU). In an effort to remedy the issue and restore communications, the technicians connected the local substation network, which was intentionally isolated from other networks by design, to the corporate network in order to provide remote IP access to the support staff. The technicians left the network connection in place, thinking that a server refresh of the devices might reestablish communications between the protective devices and the RTU.

URE created CCAs when it connected the substation's local network to the corporate network, establishing remote IP access to the substation's Cyber Assets. The substation's Cyber Assets, which were essential to the operation of the Critical Asset but had not been previously able to communicate outside of the substation network, were able to communicate outside the substation network as a result of the technicians' actions. Thus, the substation's Cyber Assets became CCAs. URE's CCA list did not account for these CCAs when URE established the IP connection between the two networks. The technicians' actions also created a condition in which the newly created CCAs existed outside of a documented ESP and were not protected within a documented PSP.

Approximately one week later, URE's IT department discovered this violation when it detected a duplicate IP conflict. URE dispatched technicians to the site on the same day, and the technicians removed the connection between the local substation network and the corporate network.

SERC determined that URE had a change management process in place to ensure all changes to any CCAs were managed to meet the requirements of the CIP Standards. However, URE's technicians failed to follow the change management process in this instance.

SERC determined that URE had a violation of CIP-002-3 R3 for creating CCAs without establishing the proper ESPs and PSPs to protect them.

SERC determined the duration of the violation to be from when URE connected the local substation network to the corporate network through when URE terminated the connection.

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, when URE established remote IP access to Cyber Assets at a Critical Asset without considering and protecting them as CCAs, it increased the risk that the newly-created CCAs would be compromised or rendered inoperable. Compromised CCAs could have been used to send inaccurate or corrupt data to the EMS, which in turn could have caused the loss of monitoring and control of the BPS. However, the local substation network was connected to the corporate network for seven days. In order to gain remote access to the RTU, an individual would have required access rights to the corporate network, the IP address of the RTU, knowledge of how to establish remote access to the RTU and how to use the RTU's software; and the RTU's log-in information. In addition, URE conducted a peak case study during the timeframe that this issue existed. The modeled scenario concluded that there would have been no load dropped or overloads on any other elements of the BPS if all lines within the site had an outage.

CIP-006-1 R3 (SERC2012011433)

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

CIP-006-1 R3 provides:

> R3. 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. One or more of the following monitoring methods shall be used:

R3.1. 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.

R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

CIP-006-1 R3 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to ensure that unauthorized access attempts were reviewed immediately and handled in accordance with CIP-008. URE had a physical security plan that addressed how it would provide physical security to protect Critical Cyber Assets and non-critical Cyber Assets within the PSPs. URE utilized a PACS that would immediately send an alert for "forced entry" or "door held open" conditions at any PSP to the central alarm station, which URE monitored at all times.

URE also had a procedure that addressed unauthorized badge attempts. This procedure required URE to review unauthorized badge access attempts to PSPs. This procedure provided guidance on actions required, based on the quantity of invalid badge presentations and the access privileges granted. However, this procedure required URE to review unauthorized badge attempts on a daily basis, instead of immediately as required by the Standard.

SERC determined that URE had a violation of CIP-006-1 R3 for failing to ensure that unauthorized access attempts were reviewed immediately and handled in accordance with the procedures specified in CIP-008.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had an established process in place to review unauthorized access attempts on a daily basis. In the event of an actual unauthorized access from a forced door or a door held open, the PACS would provide an immediate alert to the central alarm station, which URE monitored at all times. URE found no malicious unauthorized badge access attempts after its daily investigations of such attempts.

CIP-005-1 R1.1 (SERC2012011434)

The purpose statement of Reliability Standard CIP-005-1 provides: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).

***

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

During the Compliance Audit, SERC discovered that URE failed to identify and document all access points to the ESP, including any externally connected communication end point terminating at any device within the ESP.

URE failed to identify serial connections into its satellite data acquisition nodes (SDN) equipment as access points. The SDN devices were comprised of CCAs and non-critical Cyber Assets within the ESP. URE identified and protected the SDN devices as CCAs and non-critical Cyber Assets as appropriate, and established ESPs around the SDN equipment by utilizing firewall pairs to manage routable communications. URE determined that each firewall pair was the access point to the established ESP. URE determined that the serial connections to each piece of SDN equipment were not routable and therefore did not consider the serial connections as access points to the ESP. The SDN devices were not dial-up modems but were leased point-to-point circuits over which non-routable protocols communicated with RTUs in the field. Remote interactive access was not enabled on the serial connections, meaning that the serial connections could not be used to control the SDN devices.

Although these SDN devices utilized serial, non-routable protocols to communicate out to RTUs and bring data into the EMS control network, they should have been considered as externally connected endpoints that constituted an access point to an ESP.

SERC determined that URE had a violation of CIP-005-1 R1.1 for failing to identify and document all access points to the ESP, including any externally connected communication end point terminating at any device within the ESP.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The SDN devices used non-routable serial connections to communicate outside of the ESP and did not have remote interactive access enabled on the serial connections, preventing the use of the serial connections to control the SDN devices. URE protected the SDN devices as CCAs and non-critical Cyber Assets, as appropriate, within the ESP. In addition, URE utilized IDS to alert on any intrusions.

CIP-007-1 R4.2 (SERC2012011435)

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

CIP-007-1 R4 provides:

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

R4.2. The Responsible Entity shall document and implement a process for the update of anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to document procedures for testing antivirus updates before deploying the signatures into production. URE's documented procedures stated that "ideally" signatures would remain on control machines for 24 hours. However, no procedure adequately defined what might trigger the entity to stop the rollout of new definitions or a rollback of faulty definitions. SERC found that URE's procedures did not address the differences between updates of only antivirus definitions and those updates that also included antivirus engine code. In addition, the documented procedures provided no timeline for implementation or indication of an acceptable gap in time between availability and installation. Instead, URE's policy stated that all Windows machines should maintain only the "latest" definitions, contradicting the documented procedure of delaying new definitions for 24 hours in a control group. Finally, SERC determined that URE was not testing antivirus signatures prior to deployment. URE instead relied on the vendor's testing of antivirus and malware prevention signatures.

Prior to the Compliance Audit, URE began requiring all available signatures to be placed into a non-production environment for a minimum of 24 hours prior to their release into the production environments for testing purposes. At that time, URE also began requiring that all results of the testing be documented and retained.

SERC determined that URE had a violation of CIP-007-1 R4.2 for failing to document and implement a process for the update of antivirus and malware prevention signatures that addressed testing and installation of the signatures.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE began requiring the documentation of testing antivirus signatures prior to deployment to the production environment.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE was implementing all software and signature updates. The required and installed signatures caused no negative operational impacts. URE had IDS in place and operational, and no issues were detected regarding defective signatures. In addition, URE had logging enabled for all Cyber Assets within the ESP, as technically feasible.

CIP-007-1 R7.3 (SERC2012011437)
CIP-007-1 R7 provides:

> R7. Disposal or Redeployment — The Responsible Entity shall establish 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.
>
> 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-007-1 R7.3 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to maintain complete records demonstrating that Cyber Assets from within the ESP were disposed of or redeployed in accordance with documented procedures.

SERC reviewed URE 's equipment decommissioning policy and found that it required any Cyber Asset being removed or replaced from an ESP to have all hardware (e.g., servers and computers) removable storage media (e.g., disks and tapes), and mass storage (e.g., hard drives) purged of any and all data associated with the Cyber Asset's former function, location, or purpose. The equipment decommissioning policy further required that all information associated with the disposal or redeployment of these Cyber Assets be maintained as a record of disposal, redeployment, or return of equipment.

URE also had two procedures that detailed how the sensitive data would be removed from Cyber Assets and how records of disposal or redeployment would be maintained. The first procedure addressed the disposal of network equipment. The second procedure addressed the disposal of all other Cyber Assets within the ESP. In addition to providing details on how confidential data should be destroyed or removed from any Cyber Asset, each procedure directed the users to maintain proper documentation of the decommissioning or redeployment.

Following the Compliance Audit, URE conducted an internal review to determine the scope of the violation. After reviewing several hundred change tickets over the course of two years, URE determined that eight employees had failed to maintain required documentation on approximately 100 change tickets in accordance with its documented procedures. Each change ticket corresponded to one Cyber Asset.

The eight employees involved in this violation failed to follow the documented procedures and capture all data for all change tickets. The eight employees omitted serial numbers or locations for Cyber Assets that were removed from service or failed to document the disposal status of the Cyber Assets.

URE stored Cyber Assets that were not needed for immediate redeployment within the secured PSP. None of the affected Cyber Assets left the custody of URE. In all cases where Cyber Assets were needed for redeployment, URE attested that it had properly sanitized all of them in accordance with its procedures.

SERC determined that URE had a violation of CIP-007-1 R7.3 for failing to maintain complete records demonstrating that Cyber Assets from within the ESP were disposed of or redeployed in accordance with documented procedures.

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 minimal and not serious or substantial risk to the reliability of the BPS. URE maintained custody of Cyber Assets at all times. In addition, URE maintained all Cyber Assets not redeployed within secured PSPs. URE attested that it properly sanitized the Cyber Assets that it redeployed in accordance with its procedures.

CIP-006-3c R1.6 (SERC2013011699)

The purpose statement of Reliability Standard CIP-006-3c provides in pertinent part: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets."

CIP-006-3c R1 provides in pertinent part:

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

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

CIP-006-3c R1.6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to follow its visitor control program for a visitor with escorted physical access to a PSP. URE's visitor control program required that any visitor be continuously escorted and remain within the line of sight of their escort at all times when the visitor is within the PSP. On the day in question, an employee with authorized physical access allowed an unauthorized cleaning contractor access into the URE control center PSP by holding the door open. The employee then failed to escort the visitor within the PSP and failed to keep the visitor within line of sight. However, the cleaning contractor signed into the visitor log book and put on the visitor lanyard as required by the visitor control program. The cleaning contractor then proceeded to swap the recycle bins inside the control center PSP.

Approximately five minutes later, a second employee with authorized unescorted physical access entered the URE control center PSP as the cleaning contractor was preparing to exit and noted that the cleaning contractor did not have an escort. The second employee immediately brought the situation to the attention of management. Management reviewed video footage and determined that the cleaning contractor, while performing his regular duty of retrieving the recycling bin, had not taken any actions counter to his assigned role for the five minutes he was unescorted within the control center PSP.

SERC determined that URE had a violation of CIP-006-3c R1.6 for failing to implement its visitor control program requiring continuous escorted access of visitors within the PSP.

SERC determined the duration of the violation to be from when the cleaning contractor entered the PSP without an escort through when the unescorted individual left the PSP (approximately five minutes).

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE control center was manned at all times. The cleaning contractor was a regular visitor into the PSP, was aware he needed to sign in on the log book and wear a visitor badge, and performed his job requirement of retrieving the recycle bin while he was unescorted. All employees with approved unescorted access to the URE PSPs received annual training on the procedure for escorting visitors, which enabled the second employee to identify the violation. The URE control center facility had on-site security officers performing regular patrols and physical security alarm monitoring. The URE control center has also been secured with defense-in-depth layered security practices including an IDS and electronic and physical access controls.

CIP-006-3c R1.6 (SERC2013011706)

CIP-006-3c R1 provides in pertinent part:

> R1. Physical Security Plan —The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
>
> ***
>
> R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

CIP-006-3c R1.6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to follow its visitor control program for a visitor with escorted physical access to a PSP. URE followed a visitor control program that required that any visitor be continuously escorted and remain within the line of sight of their escort at all times when the visitor is within the PSP.

On the day in question, four contractors were retained to perform a project within the URE control center PSP. Prior to starting the project, the URE manager met with the four contractors who would be working within the PSP and reviewed the internal procedure for escorting visitors, as well as URE's cyber security policy. An URE employee found one of the contractors out of the line of sight of his escort and immediately notified the URE manager. URE halted all work and took the four contractors into a conference room to discuss the situation and re-review the procedures for escort of

unauthorized personnel. URE learned that the contractor had stepped away from his escort for approximately 10 minutes in order to go the restroom. After this discussion, URE allowed all four contractors to re-enter the PSP to complete the project.

SERC determined that URE had a violation of CIP-006-3c R1.6 for failing to follow its visitor control program for a visitor with escorted physical access to a PSP.

SERC determined the duration of the violation to be from when the individual moved out of the line of sight of the escort through when the individual was back under continuous escort, approximately ten minutes later.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The URE control center was manned at all times, and the control center facility had on-site security officers performing regular patrols and monitoring physical security alarms. The employee who discovered the contractor outside of the line of sight of his escort followed procedures by reporting the incident to a manager. The URE control center has been secured with defense-in-depth layered security practices including an IDS and electronic and physical access controls, and URE found no issues as a result of this incident. The contractor was outside of the line of sight of his escort for approximately 10 minutes and was allowed to complete his work after the incident.

CIP-006-3c R4 (SERC2013012206)
CIP-006-3c R4 provides:

> R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> - Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> - Special Locks: These include, but are not limited to, locks with “restricted key” systems, magnetic locks that can be operated remotely, and “man-trap” systems.
> - Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.

- Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-3c R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it failed to document and implement the operational and procedural controls to manage physical access at all access points to the PSPs at all times. URE had an access approval process that required that any request for physical or electronic access to Critical Assets or CCAs be made through the access control ticketing system, where it would be documented and routed for approvals. A URE corporate facilities manager provided an emergency access override key to a new area manager with operational responsibility for a site identified as a Critical Asset. This site contained CCAs and was secured by a PSP which had a physical key that could be used in emergency situations to provide access to personnel if the card reader system was non-operational.

The new area manager had a business need for the physical key, had received the appropriate cyber security training, and had a valid PRA. However, the new area manager did not request the emergency access override key through the ticketing system, as required by access approval process. Instead, URE provided the key to the new area manager without the proper request and subsequent approval by the space owner.

Approximately three months later, during an internal compliance review effort, URE discovered this violation and submitted the appropriate request through the access control ticketing system. On the next day, the new area manager received the proper approval to possess the emergency access override key.

SERC determined that URE had a violation of CIP-006-3c R4 for failing to implement its controls to manage physical access at all access points to the PSPs at all times.

SERC determined the duration of the violation to be from when URE provided a physical access override key to a manager without proper approvals through when the manager received proper approvals to have the physical access override key.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. If the manager used the emergency access override key, it would have sent a forced entry alarm to the URE security console, and security personnel would have immediately investigated the cause of the alarm. The manager did not use the emergency access override key prior to receiving the proper approval. URE security personnel reviewed forced entry alarms and video footage from

security cameras at the PSPs for the period in question and confirmed that there had been no forced entry alarms resulting from the use of an emergency access override key during the violation period. In addition, the manager involved in this violation had a valid PRA and current cyber security training.

CIP-004-3a R4.1 (SERC2013012431)

The purpose statement of Reliability Standard CIP-004-3a provides: "Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness."

CIP-004-3a 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-004-3a R4.1 has a "Lower" VRF and a "High" VSL.

URE submitted a Self-Report to SERC stating that it failed to update the list of personnel with authorized access to CCAs within seven days of a change of access rights for a contract security guard. URE submitted a second Self-Report to SERC stating that it failed to update the list of personnel with authorized access to CCAs within seven days of a change in the access rights for a contractor. SERC determined that this violation involved the same Standard and Requirement as the first Self-Report and decided to treat the second Self-Report as an expansion of scope.

URE's compliance group discovered that a contract security guard with authorized access to PSPs had resigned on good terms. The security guard's manager retrieved the guard's access badge upon resignation. This effectively removed the guard's physical access to any PSP or facility, but the guard's access was not revoked in the access control tool until approximately two months later due to human error when entering the change in status into the human resources personnel database. As a result, URE did not update the list of personnel with access to CCAs within seven calendar days.

After this initial discovery, URE initiated an internal review of all personnel with CCA access. URE found one additional individual who was not removed from the CCA access list within seven days. An URE contractor transferred to a role not requiring CCA access. The contractor's supervisor obtained the access card from the contractor on the same day, but failed to submit the proper transfer paperwork into the human resources system that would have triggered the update of the CCA access list. URE updated the list on the same day that it discovered this instance, which was approximately two months after the contractor transferred roles.

SERC determined that URE had a violation of CIP-004-3a R4.1 because it failed to update its lists of personnel with access to CCAs within seven calendar days in two instances.

SERC determined the duration of the violation for the first instance to be from eight days after the URE security guard resigned through when URE updated its CCA access list, approximately two months later.

SERC determined the duration of the violation for the second instance to be from eight days after the URE contractor transferred to a role not requiring CCA access through when URE updated the CCA access list approximately two months later.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE collected the access cards from both individuals on the dates their respective changes in status occurred, effectively removing their access the PSP.

CIP-006-3c R1.6 (SERC2013012710)
CIP-006-3c R1 provides in pertinent part:

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

R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:

R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

R1.6.2. Continuous escorted access of visitors within the Physical Security Perimeter.

CIP-006-3c R1.6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it discovered two contractors who did not have approved unescorted physical access rights working inside a PSP without an escort.

URE utilized a contractor with approved unescorted physical access permissions to escort two other contractors into an established control center PSP to perform electrical work. The contractors did not work on or access any Cyber Assets. Both contractors were properly logged into the PSP upon initial entry using the site visitor log book. However, the authorized escort left the site for approximately 30 minutes, leaving the two escorted contractors within the site to continue working unescorted. In addition, the authorized escort left the two contractors his personal access badge so the contractors could go to and from their work truck in order to obtain tools and parts. A security guard discovered the two contractors within the PSP unescorted, immediately halted their work, and removed them from within the PSP while he located the escort that left them unattended.

SERC determined that URE had a violation of CIP-006-3c R1.6 for failing to implement its visitor control program requiring continuous escorted access of visitors within the PSP.

SERC determined the duration of the violation to be from when the escort left the two contractors without authorized unescorted access alone in the PSP through when a security officer discovered the two unescorted contractors and escorted them out of the PSP approximately 30 minutes later.

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 contractor's decision to leave two contractors unescorted within a PSP for 30 minutes with his personal access badge gave the unescorted contractors the ability to let anyone into the PSP, where unauthorized individuals could have damaged or disrupted the normal functioning of CCAs. However, on-site security recognized the unescorted contractors and

immediately ended the non-complaint situation. In addition, URE utilized an IDS and real-time monitoring and alerting of Cyber Assets within its ESPs, which would have alerted URE personnel in the event Cyber Assets were damaged or accessed.

CIP-004-1 R3 (SERC2013012712)

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

CIP-004-1 R3 provides:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.
>
> R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
>
> R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

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

URE submitted a Self-Report to SERC stating that it granted two employees unescorted physical access to CCAs without compliant PRAs on file. URE granted authorized unescorted physical access to two employees in error. The first employee was granted physical access to CCAs prior to the mandatory compliance date. Due to a data entry error into the URE tracking database used to maintain results and dates for PRAs, an invalid PRA date was entered for this employee. Because of this error, the regular periodic reviews showed that the individual was not required to renew the existing PRA.

The second employee was granted access to the URE control center. This employee received prior authorization for authorized unescorted physical access in order to perform assigned job duties, and the employee submitted a ticket to begin the process of obtaining access. This employee shared the same name as another employee who had received authorized unescorted physical access previously and had a valid and current PRA on record. As a result, once the second employee's ticket was entered to complete the prerequisite for a valid PRA, the personnel responsible for validating the PRA saw the same name with a current and valid PRA. The personnel responsible for validating the PRA therefore utilized the first employee's valid PRA results for the second employee with the same name.

URE discovered this violation approximately one month after the second employee was granted access and revoked the authorized unescorted physical access rights for both employees the following day.

SERC determined that URE had a violation of CIP-004-1 R3 for granting two employees unescorted physical access to CCAs without having compliant PRAs on file for those employees.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Both employees were long-term employees, and both employees were in good standing with URE prior to and after this violation. Both employees were approved for access and had received the proper cyber security training prior to gaining access to CCAs. The PSPs to which these employees had access were staffed at all times. In addition, URE used an IDS to alert immediately on any unauthorized access to any Cyber Assets within the ESPs.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of three hundred and fifty thousand dollars ($350,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. the violations constituted URE 's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported 17 of the violations;[4]
3. URE was cooperative throughout the compliance enforcement process;
4. URE had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. 36 out of 37 violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. 1 out of 37 violations posed a serious or substantial risk to the reliability of the BPS, as discussed above;
8. URE has agreed to several above-and-beyond measures, which SERC considered a mitigating factor in the penalty determination. SERC reported that URE has agreed to work with SERC to conduct an appraisal of its management practices;
9. URE has expended, and will expend, considerable resources in order to improve its CIP compliance efforts, including replacing its EMS, launching an access control enterprise integration project, and centralizing its monitoring of PSPs. SERC considered these efforts to be a mitigating factor in the penalty determination; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of three hundred and fifty thousand dollars ($350,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[4] URE self-reported the violations SERC201000573, SERC201000575, SERC201000576, SERC2012010717, SERC2012010718, SERC2012010953, SERC2012010954, SERC2012010998, SERC2012011007, SERC2012011117, SERC2012011161, SERC2013011699, SERC2013011706, SERC2013012206, SERC2013012431, SERC2013012710, and SERC2013012712.

Status of Mitigation Plans[5]

CIP-002-1 R3 (SERC200900394)

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

URE's Mitigation Plan required URE to:

1. implement a tool to enhance CCA identification and assessment;
2. update its CIP-002 methodology to ensure network equipment that meets the requirements of being a CCA will be correctly identified; and
3. using its updated CIP-002 methodology, reclassify some network equipment as CCAs.

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

1. a document showing the beginning of testing, initial implementation, and reporting capabilities of the tool used for enhanced CCA identification and assessment;
2. a document showing network communications hardware is taken into account from the end point to the ESP. Network devices necessary for CCA connectivity within ESPs will be deemed as CCAs. The same corresponding change is reflected for each CIP required asset category;
3. a document showing that criteria were added for the selection of network equipment at CCAs; and
4. a document showing that the CCA and non-critical Cyber Asset lists were updated through scans performed by the new tool and that network equipment was designated as CCAs where appropriate.

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

[5] *See* 18 C.F.R § 39.7(d)(7).

CIP-004-1 R4 (SERC200900399)

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

URE's Mitigation Plan required URE to:

1. perform its annual application of its methodology and analysis of systems essential to the reliable operation of control centers and determined that the application-associated Cyber Assets were not CCAs; and
2. remove the application-associated Cyber Assets from its CCA list.

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

1. a document showing a team meeting was held where changes to the CCA list were made, including evaluation of the application as a CCA;
2. a change log showing that application assets were removed from the CCA list; and
3. a Critical Asset and CCA list showing the classification of the application as a non-critical Cyber Asset.

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

CIP-009-1 R1 (SERC200900402)

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. document a separate detailed recovery plan;
2. revise the CCA recovery plan to more clearly link individual device restoration procedures to the overall recovery plan through the use of supporting documentation;
3. communicated with and train appropriate personnel on the revised plan;
4. conduct an exercise of the revised CCA recovery plan in accordance with CIP-009; and

5. finalize supporting documentation.

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

1. a test procedure that describes intent of testing the integrity of files necessary to rebuild the recovery plan at a backup location and provides the steps necessary for recovery;
2. a revised test procedure that describes low, moderate, and high impact events in which this disaster recovery (DR) test plan will be implemented;
3. a draft version of a CCA recovery plan provided to EMS management for initial review which describes that the recovery plan is structured as an umbrella EMS business continuity plan and contains guided references to EMS's individual systems device-level DR plans. The document also provides an example of actions taken during the phases of recovery and an example of recovery and restoration procedures, by location across the system;
4. a final version of a CCA recovery plan approved by EMS management, which describes that the recovery plan is structured as an umbrella EMS business continuity plan and contains guided references to EMS's individual systems device-level DR plans. The document provides an example of actions taken during the phases of recovery and provides an example of recovery and restoration procedures, by location across the system;
5. an email providing evidence that the EMS management team met and reviewed the updated EMS DR plan, and directed the EMS management team to have direct reports review the plan for readiness and implementation of the plan;
6. an email providing an example of evidence that supporting documentation for the revised EMS DR plan was updated and reviewed by stakeholders;
7. a completed test document providing evidence that a DR test was conducted in accordance with the revised and approved EMS DR plan, and system-specific revised DR test documentation;
8. minutes from a lessons learned meeting providing the details of feedback provided during the meeting, and including a list of EMS management team participants; and
9. a revised DR test template showing that the template was updated in accordance with feedback received in the lessons learned meeting.

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

CIP-007-1 R7 (SERC201000573)

URE's Mitigation Plan to address its violation of CIP-007-1 R7 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. verify that network equipment has been sanitized appropriately for disposal or redeployment; and
2. develop and implement a documented procedure for the appropriate disposal or redeployment of network equipment within ESPs.

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

1. a document showing network devices that were removed from service, including points of contact, device names, locations, removal from service date, and date sanitized;
2. a newly-developed procedure that describes procedures to be followed for the proper disposal or redeployment of IT managed network equipment; and
3. a screenshot showing the proper sanitization of network equipment removed from service in accordance with the new procedures. The screenshot shows the case submitter's comments that network equipment was wiped and restored to factory defaults, and the device was tagged as having been sanitized.

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

CIP-007-1 R1 (SERC201000575)

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

URE's Mitigation Plan required URE to:

1. review the change management process governing the network equipment within the ESP and make updates to ensure appropriate parties are aware of network changes, that changes are evaluated for significance, and that security controls testing is documented;

2. review and update the security control test plan to ensure that the security controls tests were appropriate for network equipment; and
3. update the change management process governing network equipment within the ESP specifically for documenting significant change evaluation and cyber security testing for significant changes.

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

1. a revised procedure for the change management process addressing network equipment within an ESP that establishes the criteria for significant change evaluation, testing, and documentation for IT managed network devices and defines the criteria by which this policy must be reviewed and updated;
2. an email documenting the communication of updated procedures for significant change evaluation, testing, and documentation for the IT network support group responsible for evaluation, testing, and documentation of significant network equipment changes;
3. a cyber security controls test plan that defines the cyber controls testing that must take place for IT managed network devices on the EMS network; and
4. screenshots showing an example of a change case that was executed using the updated change management procedures.

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

CIP-007-1 R3 (SERC201000576)

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

URE's Mitigation Plan required URE to:

1. evaluate and develop or refine appropriate procedures for the patch management process, including ensuring that provisions addressing the CIP-007-1 R3 documentation requirements were specifically listed in the procedures;
2. train appropriate staff on the patch assessment process, including the documentation requirements; and

3. purchase and implement an automated security patch notification service in order to alert appropriate personnel responsible for URE's patch management process when a new security patch or upgrade is available for any Cyber Asset.

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

1. a cyber security software patch and upgrade process that documents and utilizes a standardized methodology for managing security advisory notifications and recommended code/software changes on networking equipment installed throughout EMS data networks and includes the requirements for evaluation and documentation of security advisories and patches;
2. an EMS patch management policy that establishes a standardized methodology for managing changes and patch updates and a change log that shows the annual review of this policy;
3. an email showing that the security group part of the of the code review team met and reviewed and trained on the changes and updates to the cyber security software patch and upgrade process. The email also shows that the group met and performed an annual review of the process; and
4. a screenshot showing that URE has purchased and employed an automated security patch notification service, and depicting the asset list configuration.

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

CIP-004-1 R3 (SERC200900599)

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

URE's Mitigation Plan required URE to:

1. review the access privileges for the contractor in question;
2. conduct a review of PRAs for other contractors and vendors with access to CCAs to confirm that each PRA had been updated within seven years;
3. modify its background assessment confirmation process so that actual PRA documentation, not just the PRA completion date, is reviewed by personnel prior to CCA access being granted;

4. conduct a periodic review of actual PRA dates to ensure approaching seven-year expirations are identified; and
5. approve an update to the CIP-004 R4 cyber security access program documentation, which includes language regarding the annual review of background check records to ensure individuals that were approaching a seven-year background check renewal are identified.

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

1. a copy of PACS system logs showing that a contractor's physical access was revoked;
2. an attestation from the URE compliance manager that a review of PRAs for other contractors and vendors with access to CCAs had been conducted and found no other issues;
3. a revised PRA program that states that contract administrators receive the background check results from a URE background check provider, and must then forward those results to human resources for approval.; and
4. an updated cyber security access program document that included language regarding the annual review of background check records to ensure individuals are identified that are approaching a seven-year background check renewal.

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

CIP-002-1 R3 (SERC201000609)

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

URE's Mitigation Plan required URE to:

1. produce an updated Cyber Asset listing on a quarterly basis that includes ESPs, all interconnected CCAs and non-critical Cyber Assets within the ESP, all electronic access points to the ESP, and the Cyber Assets deployed for access control and monitoring of those access points;
2. identify and evaluate a tool that helps identify assets within ESPs; and

3. configure and deploy a tool to produce input for the process to update the lists of Cyber Assets within ESPs.

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

1. a CCA list change log providing evidence of the routine review and updating of the URE CCA list at least quarterly, which includes ESPs, all interconnected CCAs and non-critical Cyber Assets within the ESP, all electronic access points to the ESP, and the Cyber Assets deployed for access control and monitoring of those access points;
2. a revised CCA list update and review procedure that states that the CCA list will be reviewed quarterly and updated as needed, and clarifies that the CCA list includes CCAs, non-critical Cyber Assets, Physical Security Perimeters, ESPs, and Access Control Assets. The document's change log provides a record of these changes;
3. a document providing evidence that the entity has successfully evaluated and implemented the deployed tool to assist in the identification of assets on the network within ESPs, and shows the network scan results during the first week of implementation of the tool; and
4. a screenshot showing the deployed tool and the network capture of Cyber Assets within ESPs to be used to produce input into the process of updating the list of non-critical Cyber Assets and CCAs, thereby demonstrating successful configuration and deployment of the tool.

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

CIP-005-1 R2.2 (SERC201000611)

URE's Mitigation Plan to address its violation of CIP-005-1 R2.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. execute a CIP firewall project that will redesign the transport network;
2. replace and retire its current legacy EMS resulting in the implementation of fully explicit permissions at each access point, thereafter conducting training and testing as necessary.

URE's Mitigation Plan is scheduled for future completion.

CIP-005-1 R4.5 (SERC201000612)

URE's Mitigation Plan to address its violation of CIP-005-1 R4.5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. begin storing results of the CVA on a highly available storage area network that is also backed up to tape; and
2. migrate to a new CVA tool that will allow the entity to store and report on historical results.

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

1. CVA results showing that the PDF reports generated by the new CVA tool are being stored on a network attached file store that is backed up and are not being stored solely in the CVA tool and also showing that the CVA documents were stored in that directory; and
2. a screenshot with the historical listing of CVAs using the new CVA tool and showing when URE began use of this tool in production CVAs.

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

CIP-005-1 R5.2 (SERC201000613)

URE's Mitigation Plan to address its violation of CIP-005-1 R5.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update its EMS change management policy to include a requirement to update documentation to reflect the modification of the network or controls within 90 calendar days of the change;
2. produce an updated Cyber Asset list quarterly to include ESPs, all interconnected CCAs and non-critical Cyber Assets within the ESP, all electronic access points to the ESP, and the Cyber Assets used for access control and monitoring;
3. evaluate and employ a tool to assist in identifying assets within ESPs; and

4. configure and deploy the tool to produce input for the process of updating the lists of Cyber Assets within ESPs.

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

1. a revised change manage policy that requires that, if any change to a CCA or non-critical Cyber Asset system or controls requires corresponding updates to EMS documentation (policies, procedures, standards, and so forth), those updates must be completed within 30 calendar days of the system or control change;
2. a revised CCA list update and review procedure that requires that the CCA list include the CCAs, non-critical Cyber Assets, PSPs, ESPs, and access control assets, and that the CCA list be reviewed quarterly and updated as necessary;
3. a change log for the CCA list showing the routine review and updating of the CCA list at least quarterly and showing that each version includes a description of the change and the author;
4. an asset inventory produced by the new tool used to identify assets within ESPs showing the device type and IP address and including fields for device model, chassis serial number, and version; and
5. a screenshot from the tool used to identify assets within ESPs showing the ESPs with site names for asset identification.

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

CIP-006-1 R1.8 (SERC201000614)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change the local administrative account passwords;
2. update its access control monitoring (ACM) procedures to include a request for administrative account password changes annually;

3. develop a document to certify that ACM Cyber Assets are cleaned according to existing processes; and
4. implement a single instance of the access management system to manage access to all existing applicable CCAs.

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

1. emails demonstrating successful administrative password resets on access control servers;
2. updated account management guidelines requiring changes to the administrator account password annually;
3. a hardware equipment redeployment and disposal reference document showing the process to clean access control and monitoring Cyber Assets;
4. a hardware equipment redeployment and disposal voucher showing the checklist/voucher used to document that the access control asset device was cleaned pursuant to the existing process;
5. a procedure showing how to remove all data from all BIOS accessible drives resulting in permanent data loss;
6. a project scope statement showing the project implementation of the single instance of the access management system for existing applicable CCAs;
7. a project plan showing the project completion of the single instance of the access management system for existing applicable CCAs; and
8. a CIP physical access workflow showing the workflow process of the central administrator who is responsible for implementing the physical access process.

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

CIP-006-1 R6 (SERC201000615)

URE's Mitigation Plan to address its violation of CIP-006-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to updated its annual testing program to include a more thorough inspection of access points that included testing manipulation of request-to-exit sensors from outside

of the PSP, testing attempts to circumvent PSP access controls that do not require the use of force, and evaluation of PSP penetrations that are vulnerable to exploitation.

URE certified that the above Mitigation Plan requirement was completed. As evidence of completion of its Mitigation Plan, URE submitted a site-specific assessment from the physical security plan showing the new intrusion testing section, testing accounts for attempts to circumvent PSP access controls that do not require the use of force, evaluation of PSP penetrations that are vulnerable to exploitation, and testing accounts for manipulation of REX sensors from outside of the PSP.

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

CIP-007-1 R1 (SERC201000616)

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

URE's Mitigation Plan required URE to:

1. review the criteria for identifying a significant change and make updates as appropriate to ensure that guidance was clear;
2. review its security control testing process and make updates as necessary to ensure that guidance was clear;
3. enhance the appropriate change management tool to identify discreetly the devices associated with significant changes; and
4. re-emphasize significant change and security controls testing requirements with personnel responsible for evaluating changes and conducting security controls testing. Retention of test results is accomplished as part of the change management process. The test results are either saved directly in or referenced in the change management tool and are required as a part of the process.

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

1. an updated significant change review and evaluation document showing the devices, patches, and other changes that either are or are potentially a significant change. It also shows that questions were added that, if answered "yes," would indicate that a change was significant;

2. an updated change management procedure showing that, as a part of the approval of a change request, a determination must be made regarding security control testing using the significant change review and evaluation form;
3. a security controls test plan that shows information needed for significant changes;
4. a document showing significant change tracking which shows the change management tool; the tool adds device tracking capability and the ability to identify discreetly devices associated with significant changes; and
5. a record of personnel training sessions with attendees.

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

CIP-007-1 R2 (SERC201000617)

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

URE's Mitigation Plan required URE to:

1. convert the documentation for all ports and services from blacklists to whitelists for all Cyber Assets;
2. use whitelists for required security controls testing; and
3. create a procedure which will address the development and maintenance of whitelists.

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

1. a progress remote on the EMS whitelist showing that URE updated SERC on its mitigation plan progress;
2. a spreadsheet showing evidence of port whitelisting;
3. a document showing evidence of the network device ports whitelists;
4. a document showing scans for security controls testing are consistent with the established whitelists and showing that whitelists are in use;

5. a document showing a firewall/router upgrade of network hardware and showing port scan results with a comparison against the baselines;
6. a document showing the updated procedure and policy for creating and updating whitelists;
7. a document showing training was completed with the appropriate resources. The training session provided a review of the EMS ports and services procedure and the acceptable forms of documentation; and
8. a document showing that whitelists are being created or updated in accordance with the new EMS port and services procedure. This document is maintained to list those ports and services that have been authorized (whitelisted) on each device type.

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

CIP-007-1 R5.3.3 (SERC201000618)

URE's Mitigation Plan to address its violation of CIP-007-1 R5.3.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the user account management policy password requirements to include changing user passwords at least annually; and
2. configure a password-aging technical control for user accounts in the active directory.

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

1. an updated user account management policy requiring that passwords be changed annually;
2. a document showing the password-aging technical control that requires passwords be changed annually. This control was implemented though the group policy editor and the maximum password age was set to 365 days; and
3. an email showing notification to users that the user account management policy was updated to require that passwords be changed annually.

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

CIP-007-1 R6.4 (SERC201000619)

URE's Mitigation Plan to address its violation of CIP-007-1 R6.4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install logging equipment;
2. migrate and test existing server and application logging on the newly installed logging equipment;
3. migrate and test existing network gear logging on the newly installed logging equipment; and
4. complete a full switchover to the newly installed logging equipment.

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

1. a document showing that logging of production equipment was occurring since the installation of the logging equipment and a summary of events (logs) since installation;
2. a document showing four terabytes were allocated for the logging equipment in order to allow for 366 days of application log storage;
3. a screenshot showing cyber devices configured for logging in the logging equipment;
4. a report generated by the logging equipment showing that it was successfully logging devices; and
5. a document showing that the logging equipment had been tested and implemented.

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

CIP-007-1 R8.4 (SERC201000620)

URE's Mitigation Plan to address its violation of CIP-007-1 R8.4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. begin storing results of the CVA on a highly available storage area network that is also backed up to tape; and
2. migrate to a new CVA tool that allows the entity to store and report on historical results.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a CVA results and storage report showing the CVA tool listing of vulnerability assessments and a screenshot of the saved and backed-up PDF copies of all CVA reports generated by the CVA tool.

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

CIP-004-3 R2 (SERC2012010717)

URE's Mitigation Plan to address its violation of CIP-004-3 R2.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. train the contractor with the newer version of the NERC CIP cyber security training;
2. review all contractors with NERC CIP access to ensure they have completed current year training; and
3. release the next version of the cyber security training to align the version of the training with the beginning of each calendar year.

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

1. a screenshot showing verification of completion of cyber security training by the contractor at issue ;
2. an access review document showing that all users eligible for access to CCAs successfully completed the cyber security training hosted in the web-based application used by URE. This access review also shows that all contractors without a company-issued network ID that have access to CCAs have successfully completed cyber security training;

3. a training assignment notification example;
4. a cyber security training roster showing all of the users who were assigned the cyber security training in the web-based training application used by URE ; and
5. a screenshot showing that the next version of the cyber security training was uploaded to the web-based application used by URE to administer annual NERC CIP training.

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

CIP-004-3 R4 (SERC2012010718)

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

URE's Mitigation Plan required URE to:

1. correct the badge clearances for the two contractors;
2. train a new, single, system-wide team of dedicated CIP access administrators and their backups on CIP access requirements and the clearance administration processes;
3. move access control administration of all CIP perimeters administered on multiple servers to a centralized access control server, which separates general non-CIP building access from NERC CIP PSP access for all URE facilities; and
4. establish a single, system-wide team with the primary responsibility for managing clearances to NERC CIP PSPs, which will separate access provisioning for CIP and non-CIP access and allow CIP perimeter clearances to be handled solely by the new single system-wide team.

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

1. an access control application journal showing that improperly assigned clearances for two individuals were removed and their badges were disabled;
2. a meeting notice showing that meetings were conducted between compliance, the single, system-wide team of dedicated CIP access administrators, security, and EMS management to review CIP access requirements and the new CIP clearance administration process;

3. a workflow that provides descriptions of the newly established roles of central access control administrators and their responsibility for central administration of CIP physical access on a day-to-day basis. The document also depicts the new process for access grants done solely by the central access control administrators after NERC CIP background checks and training, and manager approval has been verified;
4. a project scope statement that describes a project to implement a single CIP access control solution for managing physical access to CCAs and details how the new process for all CCA physical access will be managed in the new single access control system;
5. a project plan providing an overview of the project plan and milestones, as well as evidence that this project was completed and closed out;
6. a screenshot showing that the physical access in the new access control system was moved to the single access control system; and
7. a document showing the transition from decentralized access administration to a centralized access control team responsible for managing the CIP clearance grant and revoke process on a day-to-day basis.

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

CIP-006-3c R5 (SERC2012010953)

URE's Mitigation Plan to address its violation of CIP-006-3c R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct security monitor refresher training on the importance of properly monitoring CIP perimeters, and provide additional refresher training on the proper steps to alert management and IT support in the event of application or monitoring workstation functionality issues; and
2. update its security officer post orders to include more detailed instructions on responding to monitoring workstation and application issues.

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

1. an email detailing the security officer refresher training conducted to re-emphasize with officers and monitors the importance of properly monitoring CIP perimeters and any associated alarms, and to train personnel on updated procedures in the security officer post orders for responding to technical or application functionality issues of the access control monitoring application. The email also provides a roster of those personnel present for the refresher training; and
2. updated security officer post orders that provide updated guidance to security officers and monitors on proper procedures for responding to technical issues related to the systems used in the access control and monitoring of PSPs.

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

CIP-006-2 R2.1 (SERC2012010954)

URE's Mitigation Plan to address its violation of CIP-006-2 R2.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. reallocate the PSP perimeter doors from the subject panel to an alternate panel that was protected from unauthorized physical access within an established PSP; and
2. update its physical security plan to include clarifying language and additional physical security measures for physical site surveys and testing to ensure accountability of all access control assets within an established PSP.

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

1. a work order showing a request for work to install a new access control panel within a PSP, and for rewiring and programming in order to move the cabinet door configurations from the existing panel not within a URE PSP to this new panel within the PSP;
2. a site specific assessment within the physical security plan showing that the access control asset for the PSP is now the new panel, which is within the URE PSP;
3. a physical site survey with clarifying language added to be clear how to answer the question "Do the Access Control Assets (server and panel) reside within a Physical Security Perimeter?" and showing the changes made to the physical site survey template; and

4. a physical site survey comparing the previous version with the new version.

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

CIP-006-3c R4 (SERC2012010998)

URE's Mitigation Plan to address its violation of CIP-006-3c was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. re-train asset owners or their designee(s) with responsibility for protected site key management on key control procedures for personnel terminations or transfers;
2. replace all URE lock cores at protected sites, rendering currently issued or lost keys invalid for use;
3. narrow the scope of personnel authorized for URE protected site physical key access;
4. re-train the remaining personnel authorized for URE protected site physical key access on the process for surrendering physical keys upon termination or transfer; and
5. enhance the key administration process by implementing additional internal controls by providing URE compliance oversight of the key administration process.

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

1. a document showing that the URE asset owners or their designee(s) were re-trained on key control procedures;
2. a document showing the CIP-006 key control procedure used to re-train the asset owners or their designee(s) on protected site physical key control procedures;
3. a document showing the completion dates of the replacement of the URE protected sites physical key cores;
4. a timesheet for the individual who completed the key core replacement of the URE protected sites physical key cores;
5. an invoice showing the packing list of key cores received from the vendor for the key core replacement of the URE protected sites;

6. a document showing the narrowed scope of personnel authorized for URE protected site physical key access that were re-trained on the process for surrendering physical keys upon termination or transfer;
7. a document showing the CIP-006 key control procedure document used to retrain the personnel authorized for URE protected site physical key access on the process for surrendering physical keys upon termination or transfer; and
8. an email showing a meeting with the URE compliance manager and asset designee for URE protected sites physical keys to implement additional internal controls to enhance the key administration process.

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

CIP-006-3c R4 (SERC2012011007)

URE's Mitigation Plan to address URE's violation of CIP-006-3c R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. adjust the hinges on the door and trim the door frame to prevent the door from sticking;
2. test the door to ensure it was functioning properly; and
3. disseminate an awareness message to individuals that worked in the affected PSP to be diligent in recognizing and reporting to management any similar types of access control failures.

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

1. a door repair work order showing that the elevator lobby door for the trader floor was repaired and that the hinges were adjusted and the door was trimmed;
2. an attestation from the security services coordinator that the door in question was tested multiple times and the door was functioning properly; and
3. an email from the manager alerting employees to the problem and instructing the work group to remain vigilant and report any potential problems with access doors to management as soon as discovered.

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

CIP-006-1 R1.1 (SERC2012011008)

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

URE's Mitigation Plan required URE to:

1. install supplemental metal framework barriers or otherwise seal the PSP openings at the URE sites with solid material;
2. re-examine all PSPs in URE's facilities to ensure that each of the installed barriers were compliant with the CIP Reliability Standards and remediate any issues identified;
3. install metal framework barriers in the facility that was identified during the Compliance Audit and have security inspect the work to ensure that it was compliant with the CIP Reliability Standards;
4. conduct follow-up inspections of all PSPs to ensure that previously addressed gaps were properly and sufficiently remediated; and
5. remediate any newly-identified gaps found during the follow-up inspections.

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

1. documents and photographs demonstrating that the gaps identified by URE in its PSPs had been remediated, that follow-up inspections had been conducted, and that any newly identified gaps had been remediated;
2. documents and photographs demonstrating that the gaps identified by the SERC audit team at URE facilities had been remediated; and
3. documents and photographs demonstrating that all of the PSPs had been inspected for gaps in the PSPs, that any previously-identified gaps had been remediated, and that any newly-identified gaps had been remediated.

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

CIP-002-3 R3 (SERC2012011117)

URE's Mitigation Plan to address its violation of CIP-002-3 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. disconnect the device connected to the substation network and remove the network cable;
2. train the relevant engineers on CIP processes and procedures to ensure that they fully understand their importance;
3. develop new signage to reassert who must be informed prior to work being performed in Critical Asset substations. This signage was placed at all Critical Asset substations;
4. verify that the remote connectivity did not introduce any additional security concerns at the substation; and
5. disable the connections to the substation's special protection devices in the electronic control system for substations.

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

1. an email from the substation senior technician showing that the device in question was disconnected from the substation network and the network cable was removed to prevent reoccurrence of the same incident;
2. image files showing that additional signage was developed and implemented at the substation with clarifying language that reads "Do not change ANY network connection on this device for ANY reason." The images provide examples of the labels installed on the substation equipment to reassert compliance at the substations and direct personnel to the appropriate contacts for questions;
3. an email showing that CIP processes and procedures were reviewed with the field engineer responsible for the incident and demonstrating evidence of the training agenda and attendance record for the CIP substation re-training conducted for the two relevant engineers on change control procedures at critical substations;
4. an agenda from the substation training showing that training was conducted and highlighting the portions of the agenda where the two relevant engineers were trained to reinforce CIP

compliance at substations. Training topics included the definition of a critical substation, why the substations are disconnected, and who needs to be contacted prior to changes being made at the substation;

5. a screenshot and description of the tool used to determine variances in a given set of configuration files at the substations, substation configuration files captured prior to the incident, substation configuration files captured after the incident, and the analysis completed which confirmed no security concerns were introduced; and
6. an application screenshot and description showing that the devices for the substation were disabled in the electronic control system for the substation. By disabling the connections, the connections are still visible in the application, but they are unusable.

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

CIP-002-3 R3 (SERC2012011161)

URE's Mitigation Plan to address its violation of CIP-002-3 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. unplug the local network at the substation from the corporate network;
2. install physical port locks on appropriate assets to deter unauthorized changes;
3. add clarifying language to signs and tags, as appropriate, in the substation to alert personnel to follow the change management process at this facility under all circumstances; and
4. verify that the remote connectivity did not introduce any additional security concerns at the substation.

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

1. a photo showing that URE personnel disconnected the RTU and human machine interface from the corporate network;
2. a photo showing the port lock and then photo of port lock installed by URE;
3. a photo of cable labels and signs used to instruct and prevent any future network connections;

4. an email from a URE engineer attesting that that the mitigating items outlined in this mitigation plan were completed, with the dates of completion and a description of the impacted devices; and
5. a screenshot showing a comparison of the pre-incident and post-incident settings, concluding that no changes were made.

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

CIP-006-1 R3 (SERC2012011433)

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. complete updates to the physical security plan, physical access procedure, and physical site assessment to address unauthorized physical access attempts;
2. disseminate user awareness and training messaging on changes to the physical security plan and the physical access procedures to address unauthorized physical access attempts;
3. complete updates to security officer post orders and conduct training on new procedures for responding to unauthorized physical access attempts;
4. document and test new technical configuration changes necessary for alarming on unauthorized physical access attempts; and
5. implement the technical solution on the various operating company partitions of the PACS system.

URE's Mitigation Plan is scheduled for future completion.

CIP-005-1 R1.1 (SERC2012011434)

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

URE's Mitigation Plan requires URE to:

1. review the list of CCAs and non-critical Cyber Assets to identify devices with externally connected serial communication end points terminating within the ESP; and
2. document the serial interfaces as serial access points to the ESP in the applicable lists.

URE's Mitigation Plan is scheduled for future completion.

CIP-007-1 R4.2 (SERC2012011435)

URE's Mitigation Plan to address its violation of CIP-007-1 R4.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a revised antivirus testing procedure that will provide evidence for testing antivirus updates prior to the release of the updates to the production environment;
2. train appropriate staff on the revised antivirus testing procedures and policy; and
3. implement the revised antivirus testing procedures.

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

1. an antivirus/malware procedure and policy showing the completed procedure and policy for testing antivirus updates prior to the release of the antivirus update to the production environment;
2. a document showing the completed training of the appropriate staff on the revised EMS antivirus/malware policy and procedure; and
3. a document showing the implementation of the antivirus/malware policy and antivirus/malware procedure. Each document demonstrates that antivirus signatures were deployed to a test group prior to being released to production.

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

CIP-007-1 R7.3 (SERC2012011437)

URE's Mitigation Plan to address its violation of CIP-007-1 R7.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify the employees not following the procedure correctly and review the procedures with those employees to reinforce compliance with the equipment disposal policy and equipment disposal procedure; and
2. re-train appropriate staff on the existing policy and procedures to reinforce compliance with the equipment disposal policy and equipment disposal procedure.

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

1. a resource training document showing that the policy and procedures were reviewed with those individuals who were not following them correctly; and
2. documents showing that appropriate staff were re-trained on the existing EMS disposal and redeployment procedure to reinforce compliance. During the retraining, the EMS equipment decommissioning policy and EMS equipment disposal procedure were reviewed and acceptable forms of disposal and documentation were discussed.

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

CIP-006-3c R1.6 (SERC2013011699)

URE's Mitigation Plan to address its violation of CIP-006-3c R1.6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct formal discussions with the three employees and set expectations for future performance; and
2. re-train all URE employees with authorized unescorted access on the escort and physical log book procedures.

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

1. documents showing the employee discussions with management in reference to future performance expectations regarding physical access to PSPs; and
2. a training handout showing the training material provided to employees with authorized unescorted access on proper escort and physical log procedures. The document includes the attendance roster of the employees for the physical access procedure training included in the previous file.

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

CIP-006-3c R1.6 (SERC2013011706)

URE's Mitigation Plan to address its violation of CIP-006-3c R1.6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct formal discussions with four contractors provided by the vendor (including the contractor who was found unescorted) and their approved escorts, and set expectations for future performance; and
2. re-train all relevant employees with authorized unescorted access on the escort procedures.

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

1. a document showing a performance discussion with contractors and IT personnel on proper escorting procedures; and
2. documents showing the training materials provided to staff and the personnel that completed the training.

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

CIP-006-3c R4 (SERC2013012206)

URE's Mitigation Plan to address its violation of CIP-006-3c R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. approve the individual for the emergency access override key in the ticketing system;
2. train the managers involved in this incident on the key control procedure; and
3. develop and communicate a guidance document to the managers who were responsible for employees with access to Critical Assets.

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

1. a document showing that training was provided to the manager involved in this violation, including training on proper request and approval practices for protected site keys and key control practices;
2. an email sent to managers of employees with access to protected assets that provided guidance on termination for cause; and
3. a document showing that a guidance document was developed for communication to managers on guidance on termination for cause of employees who have access to protected assets.

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

CIP-004-3a R4.1 (SERC2013012431)

URE's Mitigation Plan to address its violation of CIP-004-3a R4.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct an internal review of all contractors with authorized cyber access or authorized unescorted physical access to ensure the accuracy of the CCA list(s); and

2. conduct refresher training with the contractor managers who did not complete all of the required termination steps in accordance with established procedures for updating the list of personnel with access to CCAs in a timely manner.

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

1. a spreadsheet showing URE contractors and vendors with authorized cyber or authorized unescorted physical access to CCAs and their respective access rights;
2. an email showing that compliance personnel met with the employee's supervisor to discuss the voluntary termination and the proper way to notify security; and
3. an email from an URE employee stating that he met with compliance personnel to review the requirements of CIP-004 R4 and the CIP manager's access control responsibilities to add or revoke access for contractors.

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

CIP-006-3c R1.6 (SERC2013012710)

URE's Mitigation Plan to address its violation of CIP-006-3c R1.6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct a formal discussion with the contractor involved in the violation and set expectations for future performance;
2. provide contract managers with awareness communication to reiterate the importance of educating contract staff on physical access procedures and the proper escorting procedures; and
3. communicate to the vendor company management the expectation of heightened awareness and adherence to established policies regarding CIP compliance requirements.

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

1. a letter providing an incident summary and background information and a list of attendees and details of the discussion. Each attendee signed that they were present and understood the seriousness of the violation;
2. a document showing refresher training for vendor contractors that covered the cyber security policy and where it can be found, personal responsibilities, physical access, physical (visitor) log books, and escorted access;
3. a document showing that the contractor involved in the violation completed the online NERC CIP security training, including a certificate of completion;
4. a letter sent to contract managers to raise awareness of who is considered a visitor, who is an escort, the role of an escort, and what visitors must do;
5. a letter to the vendor company outlining the incident with background information and confirming a meeting;
6. a document showing preparation for a meeting with the vendor company. The document reflects the materials and facts discussed at the meeting; and
7. notes from the meeting with the vendor company, which included a narrative of the meeting objectives, an overview of NERC CIP requirements, URE policies and training, and contract review.

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

CIP-004-1 R3 (SERC2013012712)

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

URE's Mitigation Plan required URE to:

1. revoke access for the two personnel identified in the quarterly PRA and training review;
2. work with the business unit owners and system administrators of the case management system to make modifications to existing database queries to ensure reports used for PRA periodic reviews are accurate;
3. conduct an internal review of all employees with authorized cyber or authorized unescorted physical access to CCAs to verify that a completed, compliant PRA was on file for each

employee, and that accurate data regarding each assessment has been correctly entered into the case management system; and

4. conduct an internal review of the PRA process and departmental procedures, and make updates to those procedures and reporting processes to ensure initial and periodic reviews of risk assessments are accurate.

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

1. a screenshot showing the revocation of access for the two individuals;
2. screenshots showing the revised query for generating a report for periodic review of PRA criteria, and the results utilizing the new query;
3. a report from the query noted above that lists individuals and various employee and PRA criteria. This query discovered that one individual had a PRA that was not current, which URE self-reported.
4. a list of all personnel with authorized cyber or authorized unescorted physical access to CCAs and their associated PRA-related information.
5. a report showing that the individual that was identified in the revised query now has a current approved PRA;
6. an updated process document with additional steps for conducting a PRA to ensure accuracy. The document includes requirements for monthly audits and quarterly reviews; and
7. an email acknowledging that the recipients have received and understand the revised work process for PRAs.

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[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 23, 2013. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a three hundred and fifty thousand dollar ($350,000) 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. the violations constituted URE 's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported 17 of the violations, as discussed above;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SERC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SERC determined that 36 out of the 37 violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. SERC determined that 1 out of the 37 violations posed a serious or substantial risk to the reliability of the BPS, as discussed above;

[6] *See* 18 C.F.R. § 39.7(d)(4).

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

8. URE has agreed to several above-and-beyond measures, which SERC considered a mitigating factor in the penalty determination, as discussed above;
9. URE has expended, and will expend, considerable resources in order to improve its CIP compliance efforts, which SERC considered a mitigating factor, as discussed above; and
10. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of three hundred and fifty thousand dollars ($350,000) 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

REDACTED FROM THIS PUBLIC VERSION

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560	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
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	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	Marisa A. Sifontes* General Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org

Andrea B. Koch* Director of Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org	James M. McGrane* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org
*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: SERC Reliability Corporation