PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

May 29, 2014

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. 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, CIP-004, CIP-005, CIP-006, and CIP-007. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[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.

conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC201000685, SERC201000568, SERC201000569, SERC2012010884, SERC201000729, SERC2012011010, SERC201000730, SERC2012011011, SERC201000682, SERC201000731, SERC2012010586, SERC2012010860, SERC2013012360, SERC201000679, SERC201000733, SERC2012010585, SERC201000683, SERC2012009109, SERC201000678, SERC201000734, SERC201000735, SERC2012010883, SERC201000566, SERC201000736, SERC201000570, SERC201000567, SERC2012011013 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 March 17, 2014, by and between SERC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), 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.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC201000685	CIP-002-2	R2	High	$250,000
			SERC201000568	CIP-004-1	R3	Medium	
			SERC201000569	CIP-004-1	R4	Medium	
			SERC2012010884	CIP-004-3	R4	Lower	
			SERC201000729	CIP-005-1	R1:1.5	Medium	

[4] For consistency, this filing throughout uses the earliest enforceable version of the CIP Standard applicable to each violation.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC2012011010	CIP-005-1	R1	Medium	$250,000
			SERC201000730	CIP-005-1	R2:2.2	Medium	
			SERC2012011011	CIP-005-1	R3:3.2	Medium	
			SERC201000682	CIP-006-1	R1.1	Medium	
			SERC201000731	CIP-006-1	R1	Medium	
			SERC2012010586	CIP-006-1	R1	Medium	
			SERC2012010860	CIP-006-1	R1:1.8	Medium	
			SERC2013012360	CIP-006-3c	R1:1.6.1	Medium	
			SERC201000679	CIP-006-2	R3	Medium	
			SERC201000733	CIP-006-2	R3	Medium	
			SERC2012010585	CIP-006-1	R4	Medium	
			SERC201000683	CIP-006-3a	R4	Medium	
			SERC2012009109	CIP-006-3c	R6	Lower	
			SERC201000678	CIP-007-1	R1	Medium	
			SERC201000734	CIP-007-1	R2	Medium	
			SERC201000735	CIP-007-1	R3	Lower	
			SERC2012010883	CIP-007-3a	R3	Lower	
			SERC201000566	CIP-007-1	R4	Medium	

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.[4]	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2287	SERC201000736	CIP-007-1	R4:4.2	Medium	$250,000
			SERC201000570	CIP-007-1	R5	Medium	
			SERC201000567	CIP-007-1	R6	Medium	
			SERC2012011013	CIP-007-3a	R8	Lower	

CIP-002-2

The purpose statement of Reliability Standard CIP-002-2 provides in pertinent part: "Standard CIP-002-2 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-002-2 R2 (SERC201000685)[5]

CIP-002-2 R2 provides: "Critical Asset Identification — The Responsible Entity[6] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary." [Footnote added.]

CIP-002-2 R2 has a "Medium" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL).

URE submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R2. Specifically, URE failed to update its Critical Asset list to reflect the commissioning of a substation identified as a Critical Asset.

[5] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

[6] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

URE commissioned a newly identified Critical Asset but did not add it to the Critical Asset list until approximately seven months later, the same date that URE conducted the annual review. At the time of the violation, the newly identified Critical Asset contained no Critical Cyber Assets (CCAs) and approximately 65 Cyber Assets. The root cause of the violation was URE's misinterpretation of the requirements of CIP-002 R2. At the time of the violation, URE interpreted and documented the Standard requirement language to require that it update its lists through the annual review for the following year.

SERC determined that URE was in violation of CIP-002-1 R2 because URE failed to update Critical Asset listings after a new Critical Asset was commissioned.

SERC determined the duration of the violation to be from the date the Critical Asset was commissioned through when the Critical Asset was added to URE's Critical Asset list.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE commissioned and secured the Critical Asset in accordance with the NERC Implementation Schedule for Critical Assets. URE did have and followed its documented risk-based assessment methodology. The Critical Asset did not contain any CCAs, thereby reducing the possibility of cyber compromise and limiting the number of NERC CIP Reliability Standard requirements applicable to it.

CIP-004

The purpose statement of Reliability Standard CIP-004 provides:

> Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-004-1 R3 (SERC201000568)[7]

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. 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 an employee was granted authorized unescorted physical access to a Physical Security Perimeter (PSP) without having a personnel risk assessment (PRA) performed.

URE granted authorized unescorted physical access to a single PSP to a single individual. URE removed this access approximately eight months later. URE stated that the individual had no need for physical access and did not enter or attempt to enter the PSP during this time. The individual completed the

[7] URE's violation applies from Version 1 through Version 2 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

annual URE CIP training approximately four months prior to being granted authorized unescorted physical access and did not have electronic access to CCAs. URE's processes and procedures related to physical and electronic access adequately addressed the requirements of CIP-004 R3. The violation involves 0.25% of the total individuals with access to PSPs.

SERC determined that URE was in violation of CIP-004-1 R3 because it failed to perform a PRA for one employee within 30 days of granting authorized unescorted physical access to CCAs.

SERC determined the duration of the violation to be from thirty days after physical access was granted through when access was revoked.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This individual did not have electronic access to CCAs. In addition, this individual was in good standing with URE and completed the annual URE CIP security training before receiving access. The individual never attempted to gain physical entrance into the PSP. The violation involved less than 1% of the total individuals with access to PSPs at the time of the violation.

CIP-004-1 R4 (SERC201000569)[8]

CIP-004-1 R4 provides:

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

[8] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

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

URE submitted a Self-Report to SERC stating that a local account was not removed from two network devices within seven days as required by CIP-004-1 R4.

Specifically, a local user account with administrative privileges was not removed from two network devices for approximately 22 months after the individual associated with that account no longer required electronic access to CCAs. SERC determined that URE failed to maintain its access lists for personnel with authorized electronic access to CCAs.

While SERC was assessing the violation reported in the Self-Report, the SERC audit team discovered one additional instance of noncompliance, and URE self-reported one additional instance of noncompliance involving the same Standard and requirement. SERC treated these additional instances as an expansion of scope of the violation addressed herein. Following a Compliance Audit, a SERC audit team reported a violation of CIP-004-2 R4.1. URE failed to update its authorized unescorted physical access list within seven days as required. Specifically, one manager had unescorted physical access that was revoked, but URE failed to update its access list until approximately two months later. URE failed to maintain its access lists for personnel with authorized unescorted physical access to CCAs.

URE self-reported an additional noncompliance with CIP-004-3 R4. An individual with unescorted physical access to an identified PSP retired. URE personnel requested revocation of the individual's access on the next day, but failed to revoke unescorted physical access to the PSP until nine days after the request. URE failed to revoke access to CCAs within seven calendar days for personnel who no longer required such access.

SERC determined that URE was in violation of CIP-004-1 R4 for failing to remove unneeded access to CCAs within seven days and for failing to maintain access list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs.

SERC determined the duration of the violation for the first instance to be from when the Standard became mandatory and enforceable on URE through when access was removed from switches. SERC determined the duration of the violation for the second instance to be from seven days after access was removed through the date the access list was updated. SERC determined the duration of the violation for the third instance to be from seven days after the individual retired through the date the lists were updated.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Each of the personnel involved had the required CIP cyber security training and completed

PRAs. Each of the personnel involved were in good standing with the company, and none required access revocation because of a for-cause termination.

CIP-004-3 R4 (SERC2012010884)

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

URE submitted a Self-Report to SERC stating that it granted two individuals access to a PSP without authorization from the designated authorizing officials pursuant to the established internal policy.

URE became aware of this occurrence while conducting a quarterly review. According to URE, the two individuals had access to the PSPs for approximately 55 days.

URE's internal policy requires authorized personnel to submit an online request and acquire approval by the designated officials for that PSP. Access managers are those who can authorize a request for unescorted access to a controlled URE facility. Access managers are typically plant managers, regional managers, or other responsible persons who assure only those individuals with an appropriate business need will be granted access.

URE did not submit an online request for approval for these two individuals, nor did the individuals receive permission by the authorized officials prior to receiving access. Due to the automated nature of the process, the failure to submit an online request resulted in the list of personnel with unescorted authorized cyber or authorized unescorted physical access to CCAs not being updated within the required period.

The two individuals who had access to the PSP without authorization from the access manager were the chief executive officer and a vice president. Both individuals had a completed PRA and otherwise met the requirements for CCA and PSP access.

SERC determined that URE had a violation of CIP-004-3 R4 for failing to follow its PSP access policy, which in turn resulted in a failure to maintain the list of personnel with authorized cyber, or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs.

SERC determined the duration of the violation to be from when access was granted to the two individuals without permission from the designated officials through when URE revoked access to the PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The two individuals at issue had received PRAs and cyber security training and had approved access to other PSPs. The violation was restricted to less than 1% of the individuals with PSP access at the time of the violation.

CIP-005-1

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

CIP-005-1 R1: R1.5 (SERC201000729)[9]

CIP-005-1 R1 provides:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

[9] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

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

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

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

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

SERC conducted a compliance Spot Check of URE. SERC included an audit detail letter in which SERC notified URE that CIP-005-1 R1 would be in scope during the scheduled Spot Check.

The Spot Check team reported that URE did not afford protective measures for assets used in the electronic access control and monitoring (EACM) of the Electronic Security Perimeters (ESPs), a violation of CIP-005-1 R1. Specifically, URE did not identify and protect all Cyber Assets deployed for the access control and monitoring of the ESPs.

During the Spot Check, SERC discovered that URE contracted with a managed security service provider (MSSP) to collect, identify, validate, and escalate events and monitor access points to URE's ESPs. In order to perform the contracted services, the MSSP located certain monitoring devices at URE's facilities. Those monitoring devices gathered information and sent it via secure channels to the MSSP's central servers, which were not located at URE's facilities. Because of this arrangement, the devices located at URE's facilities and the MSSP's central servers are EACM devices, and URE must afford them the protections listed in CIP-005-1 R1.5.

SERC analyzed the contract under which the MSSP performed services for URE and determined that the contract with the MSSP did not ensure that the MSSP's devices used in the access control and monitoring of URE's ESPs were afforded the protections listed in CIP-005-1 R1.5. In addition to URE's

failure to ensure contractually that the MSSP located the EACM devices within a PSP, URE also failed to provide evidence that it had provided the EACM devices with the required protections.

SERC determined that URE was in violation of CIP-005 R1.5 because it failed to provide evidence that it provided the required protective measures to Cyber Assets used in the access control and monitoring of the ESPs.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE allowed CCA monitoring information and EACM devices outside of its established ESPs, increasing the likelihood of compromised information and devices. URE did have protections in place to mitigate the potential risk. The devices in question were located within a restricted area with some physical security controls in place, including security cameras that monitored the area 24 hours a day, seven days a week, and card access systems that provided logging and monitoring. The MSSP provided URE with a description of the security controls in place to protect the affected EACM devices from unauthorized access, including, among other things, training for MSSP personnel and testing to ensure that changes and updates did not degrade security controls.

CIP-005-1 R1 SERC2012011010[10]

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

SERC conducted a Compliance Audit of URE. During the Compliance Audit, SERC discovered URE failed to identity field devices serially connected to an ESP as access points to the ESPs. Additionally, URE employs intrusion detection systems (IDS) using network span (or mirror) ports which cross the ESP, providing another type of "communication" link, the endpoints of which must be considered access points to ESPs.

URE utilized field devices that are serially connected to modems that communicate and ultimately terminate at a CCA located inside of the ESP. The serial devices use asynchronous and non-routable communication that is converted into a digital format at the CCA (a communication front-end processor). Therefore, this configuration requires the identification and documentation of an access point to an ESP pursuant to CIP-005 R1.

[10] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

Additionally, URE had implemented IDS devices that use network switched port analyzer (SPAN or mirror) ports to transfer network traffic to the IDS devices for analysis. URE configured these ports only to monitor network traffic. For all communication endpoints terminating at any device within an ESP, however, an access point must be identified. URE did not identify the connection across the ESP boundary as an access point. Since the configuration did not allow any external communication to come into the ESP via the SPAN port, and only permitted data to flow out of the ESP, URE believed that it did not need to identify an access point. Despite this configuration, however, URE should have identified access points for this connection to the ESP.

SERC determined that URE was in violation of CIP-005-1 R1 because URE failed to identify and document the ESPs and all access points to the ESPs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until the present. URE's mitigation plan for this violation is intended to create a new hierarchal network architecture based upon industry standards for data centers, eliminate the SPAN ports, and prepare URE for compliance with the controls required by CIP-005-5.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The unidentified field devices were serial devices that did not use a routable protocol, and the network switched port analyzer was configured to monitor network traffic only. URE had procedural controls in place for ESP access point management, logging, monitoring, and change control and testing of significant changes. The ESPs where the devices resided utilized real-time monitoring, including an IDS.

CIP-005-1 R2: R2.2 (SERC201000730)[11]

CIP-005-1 R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.

[11] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

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

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

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

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

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

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

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

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

SERC conducted a compliance Spot Check of URE. SERC included an audit detail letter in which SERC notified URE that CIP-005-1 R2 would be in scope during the scheduled Spot Check.

SERC's Spot Check team reported that URE enabled ports and services at ESPs that were not required for normal or emergency operations or monitoring, a violation of CIP-005-1 R2.2. URE's access control lists contained the justifications for open ports and services for the sampled EACM devices. Based on its review of these lists, SERC determined that URE had enabled ports and services at the ESPs that were not required for operations or monitoring, or which the source or destination did not require. Specifically, URE configured one access point, a firewall, to allow a CCA, to connect to any destination outside of the ESP without a service restriction. The documented description of the configuration stated that a "review of that access rule was needed."

SERC also determined that one of the firewalls at a URE facility allowed any URE employee with Virtual Private Network (VPN) access to connect to any destination within the facility's ESP via a network basic input/output system or the programmable logic controllers (PLC) communications port. URE failed to demonstrate why the ports and services associated with these types of access were required for normal and emergency operations and monitoring.

SERC determined that although not fully implemented, URE did have documented policies and procedures requiring it to enable only ports and services required for normal and emergency operations and monitoring. SERC determined that URE was in violation of CIP-005-1 R2.2 because at certain access points to its ESPs, URE failed to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP, and failed to document, individually or by specified grouping, the configuration of those ports and services.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until 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 failed to ensure that it enabled only ports and services required for normal and emergency operations on access points to the ESP. This could have allowed unauthorized individuals or malware intended to exploit these ports and services to establish a connection inside the ESP, potentially disrupting operations. URE has two violations included in this Settlement Agreement that contributed to the elevated risk. The first was URE's failure to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cyber security controls on all CCAs and non-CCAs (SERC201000678). The second was URE's failure to disable ports and services not required for emergency and normal operations on 174 Cyber Assets located inside an ESP (SERC201000730). URE did have protections in place to mitigate the potential risk. URE uses an access control model that denies access by default.

CIP-005-1 R3: R3.2 (SERC2012011011)[12]

CIP-005-1 R3 provides:

> R3. Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at

[12] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.

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

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

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

SERC conducted a Compliance Audit of URE (Audit). During the Audit, SERC discovered a violation of CIP-005-1 R3. URE failed to implement either an electronic or a manual process for monitoring or logging access at access points to the ESP 24 hours a day, seven days a week.

URE had six firewalls located at a single facility configured to log electronically all access attempts, configuration changes, and other high-level functions. However, due to high rates of firewall processing and filtering, the firewalls were not logging authorized and unauthorized access attempts to the ESP.

SERC determined that URE was in violation of CIP-005-1 R3.2 because it did not implement an electronic or manual process for monitoring and logging access at access points to the ESP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until 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 maintains a contract with a third-party security vendor that provide security analysis and prevention services at all times. The security vendor has monitoring devices at URE to assist in real-time monitoring of the URE ESP and is constantly monitoring the URE network for malicious activity. This includes immediate notification of detected security anomalies. Therefore, any malicious attempts on the firewalls would be subject to scrutiny despite the absence of authorized access

logging. Despite not logging for access, the firewalls were logging for configuration changes and protocol-based traffic denials, thereby providing the ability to detect and respond to malicious activity affecting the firewalls.

CIP-006

The purpose statement of Reliability Standard CIP-006 provides: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1.1 (SERC201000682)[13]

CIP-006-1 R1 provides:

> 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.
> >
> > R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.
> >
> > R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

[13] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R1.4. Procedures for the appropriate use of physical access controls as described in Requirement R3 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Procedures for reviewing access authorization requests and revocation of access authorization, in accordance with CIP-004 Requirement R4.

R1.6. Procedures for escorted access within the physical security perimeter of personnel not authorized for unescorted access.

R1.7. Process for updating the physical security plan within ninety calendar days of any physical security system redesign or reconfiguration, including, but not limited to, addition or removal of access points through the physical security perimeter, physical access controls, monitoring controls, or logging controls.

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.

R1.9. Process for ensuring that the physical security plan is reviewed at least annually.

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

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R1. Not all Cyber Assets located within an ESP resided within an identified PSP for two facilities.

On July 15, 2010, FERC approved an interpretation of CIP-006-2 R1.1 documenting a registered entity's ability to use alternate physical or logical measures to control physical access to Cyber Assets where the registered entity cannot establish a six-wall border. This interpretation included that the registered entity must submit a Technical Feasibility Exception (TFE) request that details the alternate physical or logical measures that protect the Cyber Assets.

SERC reviewed URE's physical security plans for the facilities in question and determined that the plans did require that all Cyber Assets within an ESP reside within an established secured PSP. The physical security plans did not specifically mention network cabling.

SERC learned that URE deployed alternative measures by enclosing portions of the network cabling in continuous steel conduit where it could not establish a six-wall border. URE also located the sections of the network cabling not enclosed in a conduit in a cable tray suspended above the ceiling of a hallway. Additionally, the building where the cable was located did have limited access, despite not being an identified PSP. URE failed to file a TFE documenting these alternative measures used to protect the communication links.

SERC determined that URE was in violation of CIP-006-1 R1.1 because URE failed to document alternative measures to control physical access to the Cyber Assets (network wiring) where it could not establish a six-wall border.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE filed the TFE.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had physical security controls in place, including limited access and video surveillance to the areas where the cabling is located. A metal conduit encloses the cabling, which would reduce the likelihood of physical or electronic access. The remaining cable was in a cable tray that is above the ceiling and out of plain sight.

CIP-006-1 R1 (SERC201000731)[14]

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

SERC conducted a compliance Spot Check of URE. In the audit detail letter, SERC notified URE that CIP-006-1 R1 would be in scope during the scheduled Spot Check.

The CIP Spot Check team reported a violation of CIP-006-1 R1. URE did not ensure that all the access points through each PSP were identified and did not ensure that the physical security plan reflected the actual PSP configuration.

URE had a physical security program in place prior to the mandatory and enforceable date of the Standard. This plan required a documented physical security assessment for each facility with CCAs. SERC staff reviewed the physical security assessment for two operating centers and determined that the assessment identified five access points into one of the operating centers, three into the center's

[14] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

storage area network server room, and six into the other operating center. SERC reviewed URE's PSP drawings, compared them to the applicable physical security assessment, and determined that URE failed to identify accurately and consistently the PSPs and all access points.

Specifically, SERC identified two instances where an access point to a PSP was undefined, undocumented, and without documented control measures approved in the physical security plan. In addition, the audit team identified that the physical security plan incorrectly identified a PSP boundary wall.

SERC determined that URE was in violation of CIP-006-1 R1 because URE failed to ensure identification of all the access points through each PSP, ensure that the physical security plan reflected the actual PSP configuration, and have measures in place to control entry to an identified PSP access point.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until when URE identified all access points, the physical security plan reflected the PSP configuration, and URE put measures in place to control entry to identified access points.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify all access points correctly could result in a failure to protect each access point. Failing to ensure that the physical security plan reflects the actual PSP configuration could result in the inability to implement a secure PSP and secure PSP practices. URE did have protections in place to mitigate the potential risk. URE monitors physical access using security guards and cameras and secured the facilities in question with access controls and layers of security, including card readers at the main entry points to the building and at the top of the stairwell leading to the entry to the basement PSP.

CIP-006-1 R1 (SERC2012010586)[15]

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

URE submitted a Self-Report to SERC stating it had a violation of CIP-006-1 R1. While conducting a physical security walk-down of its Critical Assets, URE identified two non-secured windows measuring greater than 96 square inches, one each at two separate sites. The window at one site was equipped with glass breakage detectors and alarms to URE's operation center. These detectors and alarms were in place since the Standard become mandatory and enforceable on URE. At the second site, the

[15] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

windows were located three stories above ground and were not easily accessible. URE, however, failed to identify these windows as PSP access points.

SERC determined URE had a violation of CIP-006-1 R1 for failing to identify all the access points through each PSP, ensure that the physical security plan reflected the PSP access points, and have measures in place to control entry to the PSP access points in question.

SERC determined the duration of the violation to be from when the Standard become mandatory and enforceable on URE through when URE had secured both windows so that they are no longer operable and/or did not measure greater than 96 square inches.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify all access points correctly could result in a failure to protect each access point. Failing to maintain an accurate physical security plan could result in the inability to implement a secure PSP and secure PSP access practices, and to secure the CCAs residing inside. URE did have protections in place to mitigate the potential risk. One window was three stories above the generating units and not easily accessible, and the window was equipped with glass breakage detectors that would trigger alarms if the glass was broken. In addition, URE monitors physical access at all times by using security guards and cameras.

CIP-006-1 R1: R1.8 (SERC2012010860)[16]

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8. URE reported that system complexity and implementation concerns regarding a system upgrade to URE's physical access control system (PACS) resulted in a system upgrade delay.

Specifically, URE failed to maintain a physical security plan that afforded all of the protections set forth in CIP-006-1 R1.8 to the URE PACS, which authorized or logged access to PSPs. URE failed to afford the protections of CIP-004-3 R3 by granting electronic access to two PACS administrators who had not been subject to the required PRA process. URE failed to afford the protections of CIP-007-3 R5.3.3 by failing to change the system control and account passwords within the specified period. URE failed to afford the protections of CIP-007-3 R2.1 by failing to document and implement a process to ensure it enabled only those ports and services required for normal and emergency operations. Specifically,

[16] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The pertinent language of the Requirement remained the same in each version.

URE opened ports and services related to remote management software to enable vendor support, but this support was not necessary for normal or emergency operations and URE did not document the justification. URE failed to afford the protections of CIP-009-3 R2 when it failed to test the physical security system disaster recovery plan for the calendar year. URE had tested this plan the year prior and the year after the missed testing. URE has not filed any TFEs for the PACS devices at issue in this violation.

SERC determined that URE had a violation of CIP-006-1 R1 because URE failed to create and maintain a physical security plan, approved by a senior manager or delegate, which ensured that Cyber Assets used in the access control and monitoring of the PSPs were afforded the protective measures specified in CIP-006-1 R1.8.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to ensure protection of Cyber Assets used in the access control and monitoring of the PSP could introduce additional vulnerabilities in the devices. In turn, the security of physical access points is degraded, potentially allowing unauthorized individuals to gain physical access to CCAs protected within PSPs. However, URE did have protections in place to mitigate the potential risk. The two administrators granted electronic access to the PACS without PRAs did undergo preliminary screening; this preliminary screening included a criminal history check and other checks designed to prevent potential risks posed by those individuals. The two individuals were and are in good standing with the company. The passwords that were not changed annually did meet the length requirements in CIP-007 R5.3 and URE had filed a TFE for its inability to technically meet the complexity requirements.

CIP-006-3c R1: R1.6.1 (SERC2013012360)

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-3c R1 for failing to log visitor access into a single PSP at two different times.

A contractor with authorized unescorted PSP access brought two visitors into the PSP at different times and failed to log their access. The issue was identified the following day when the contractor admitted that he failed to properly log the escorted visitors. The manual log used for tracking visitors at the time of the violation shows three manual entries. One entry the aforementioned contractor showed an entry at 8:30 a.m. and an exit at 2:30 p.m. The manual log entries, however, were non-sequential. In the course of its investigation, SERC discovered that the contractor made this entry in the manual log the day after escorting the visitors into the PSP.

URE provided an approved physical security plan, including provisions for visitor access management covering the two operating center facilities (the control centers). The plan requires escort of all visitors at all times while within the two operating centers. Additionally, the plan requires recording all visitor access to the PSP electronically or manually. URE reviewed both the electronic and manual logs associated with the access control and monitoring devices to the PSPs in question and discovered no other incidents.

SERC determined that URE had a violation of CIP-006-3c R1.6.1 for failing to log (manual or automated) the entry and exit, including the date and time, of visitors to PSPs.

SERC determined the duration of the violation to be from when the visitors came onsite through when the visitors left the site.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The contractor at issue did have valid access to CCAs and training on the documented visitor escorting policy. The contractor did escort the visitor while the visitor was in the PSP. URE's PSPs were secured with access controls, including electronic card readers at all access points, a security desk with guards at the main entrances to the buildings, and live 24 hour a day, seven day a week security cameras covering the areas. After reviewing other logs and video surveillance, URE determined that all other visitors to PSPs were properly escorted.

CIP-006-2 R3 (SERC201000679)[17]

CIP-006-2 R3 provides: "Protection of Electronic Access Control Systems — Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall reside within an identified Physical Security Perimeter."

CIP-006-2 R3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-2 R3. A single firewall used to protect the facility's dispatch control call center ESP was not physically located within a designated PSP.

This issue involved a single firewall that was responsible for securing and monitoring CCAs in the operating center. That firewall was located outside of the designated PSP, the communication room of the operating center. URE had an established and approved physical security plan that enforced proper use of all Cyber Assets used in the access control and monitoring of the ESP and required them to reside within an identified PSP. Physical access control devices (i.e., card readers and cameras) protected the firewall in question, which was located in an area restricted from unauthorized personnel. However, URE had not designated this restricted area as a PSP in its physical security plan. URE granted access to this area based on job function and restricted access to a subset of approximately 10 information technology (IT) support personnel in the operations center. The 10 IT support personnel that had access to the restricted area each had a completed PRA on file and had completed annual cyber security training.

[17] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. This requirement did not exist in Version 1. The language of the Requirement remained the same in each version.

Through a physical walk-down and a review of operating center and plant diagrams, URE confirmed that all other electronic access control and monitoring systems resided within identified PSPs, and that this condition did not exist in any other areas of URE.

SERC determined that URE was in violation of CIP-006-2 R3 for failing to position all Cyber Assets used in the access control and/or monitoring of the ESP in an identified PSP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable through when URE relocated the firewall to a designated PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The single firewall in question was located within a restricted area that did have physical security controls in place, including security cameras that monitored the area 24 hours a day, seven days week and card access systems that provided logging and monitoring. Access to the firewall was limited to approximately 10 trained and screened IT administrators.

CIP-006-2 R3 (SERC201000733)[18]

CIP-006-2 R3 has a "Medium" VRF and a "Severe" VSL.

During a Spot Check of URE, SERC discovered a violation of CIP-006-2 R3. URE did not ensure that all ESP EACM devices resided within a defined PSP.

SERC discovered that URE contracted with a third-party MSSP to collect, identify, validate, and escalate events and monitor access points to URE's ESPs. The MSSP did so by locating certain monitoring devices at URE's facilities. Those monitoring devices would gather information and securely send it to the MSSP's central servers that were not located at URE's facilities. Because of this arrangement, the devices located at URE's facilities and the MSSP's central servers are EACM devices and must be protected pursuant to the applicable CIP Reliability Standards, including CIP-006-2 R3. URE's contract with the MSSP did not ensure that the MSSP's devices used in the access control and monitoring of URE's ESPs resided within an established PSP, as required by CIP-006-2 R3.

In addition to URE's failure to ensure contractually that the MSSP located the EACM devices within a PSP, URE also failed to provide evidence that the EACM devices in fact were located within a PSP. Specifically, SERC determined that the servers used for management of access points to ESPs were not

[18] URE's violation applies from Version 2 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

located within an established PSP. URE did have a procedure that required identification of EACM devices and required them to be located within PSPs. URE, however, failed to implement this procedure with respect to these EACM devices.

In addition to the MSSP's EACM devices, SERC also determined that URE failed to locate some of its own EACM devices within a PSP, as required by CIP-006-2 R3. The EACM devices at issue were servers used to configure access points to ESPs and manage firewalls and routers.

SERC determined that URE was in violation of CIP-006 R3 because it failed to provide evidence that Cyber Assets used in the EACM of the ESPs were located within a PSP.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to ensure that some devices involved in the access control and monitoring of an ESP were located within a defined PSP increased the risk of unauthorized physical access to URE's EACM devices. URE did have protections in place to mitigate the potential risk. The devices at issue were located within a restricted area with some physical security controls in place, including security cameras that monitor the area 24 hours a day, seven days a week, and card access systems that provided logging and monitoring. The third-party MSSP provided URE with a description of the security controls in place to protect the EACM devices from unauthorized access. MSSP trained its personnel and performed testing to ensure that changes and updates did not degrade security controls.

CIP-006-1 R4 (SERC2012010585)[19]

CIP-006-1 R4 provides:

> R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

[19] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.

R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

CIP-006-1 R4 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it was in violation of CIP-006-1 R4 because URE did not have a manual log to record the use of an equipment elevator that served as an access point to one PSP.

URE conducted a physical security walk through of the URE operating center and determined there were no manual logging mechanisms implemented to record use of the equipment elevator lobby double doors, which is an established access point to the PSP there. Seventy individuals had access to this area during the time of the violation.

SERC determined that URE was in violation of CIP-006-1 R4 because it did not implement and document the technical and procedural mechanisms for logging physical entry at all access points to the PSP.

SERC determined the duration of the violation to be from when 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, failure to secure access points to the PSP could have allowed unauthorized personnel unescorted access without detection. URE did have protections in place to mitigate the potential risk. URE did have an alarm contact on the doors located under the equipment hatch that alarms to the URE monitoring and notification center any time the equipment elevator is used. When not in use, the elevator is located at ground level outside the PSP, and the only way to access it is through the PSP. There is a card reader located at the PSP access point which grants access to the telecommunication room where networking CCAs are located. There is an armed response team on-site 24 hours a day, seven days a week.

CIP-006-3a R4 (SERC201000683)

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

URE submitted a Self-Report to SERC stating that it had a violation of CIP-006-3a R4 because the doors to its server room and operations center were inadvertently left unlocked for approximately 7 hours and 15 minutes after a fire drill.

URE had a scheduled fire drill. At the time, in accordance with URE's physical security plan, the door locks were programmed to fail open for safety reasons in any fire drill or other emergency-related event. It was URE's standard practice to reset the alarms and locks after the completion of the drill. In this instance, the responsible individuals failed to reset the door locks to the PSP at the conclusion of the fire drill.

URE reviewed video footage and access logs to determine that the doors to the server room and operations center were unsecured for 9 hours and 19 minutes, which included the duration of the fire drill and 7 hours and 15 minutes after the drill. URE also found that two contract individuals had accessed the PSP without proper authorization during this period. The individuals at issue were

performing maintenance on lighting fixtures, and had general access into the building, but did not have authorized access into the operations center PSP. URE normally escorted these individuals into the controlled area, but in this instance, the individuals entered the PSP after scanning for badge access that was denied. The individuals' badge attempt was logged and an alarm was generated, but it was not received and responded to immediately due to the ongoing fire drill efforts.

URE had a physical security plan that required, in the event of a system failure of a PACS, the monitoring and notification center to restrict access to the PSP. However, in this instance, access was restricted only for the duration of the fire drill by placing security guards at the entry points.

SERC determined that URE was in violation of CIP-006-3a R4 for failing to implement the operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from 10:02 a.m., when the drill started and URE failed to manage physical access at all access points to the PSPs through 7:21 p.m. when URE reset the locks at the access points to the PSP at issue.

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, a failure to implement technical and procedural controls resulted in unauthorized access into the PSP at issue. Unauthorized access into a PSP could allow potential unauthorized access to the CCAs contained inside the PSP. URE did have protections in place to mitigate the potential risk. URE had multiple cameras with recorded video feeds monitoring the server room and operations center during the violation, including the scheduled fire drill and the period after the drill. URE's electronic logging was enabled and functional during the violation, including the scheduled fire drill and the period after the drill. The contractors at issue had undergone background checks and were approved for general access into the facility, although not to the CCAs within the PSP. URE's security guards visually monitored the area during the drill. No Cyber Assets within the PSP were compromised.

CIP-006-3c R6 (SERC2012009109)

CIP-006-3c R6 provides:

> R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural

mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:

- Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
- Video Recording: Electronic capture of video images of sufficient quality to determine identity.
- Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

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

URE submitted a Self-Report stating that it was in violation of CIP-006-3c R6. URE failed to record or to maintain logs of an unauthorized employee's physical access.

URE discovered that a vendor-provided custodial employee was attempting to gain entry to a card-access and biometric-controlled control center PSP with a second individual's badge. The second individual loaned the access badge to the first individual while on vacation. URE's PACS logged a biometric mismatch for the actual cardholder. URE immediately responded to the alarm, and one of URE's security personnel confiscated the badge.

This instance prompted URE to conduct an internal investigation. URE reviewed historical video surveillance and electronic and manual logs to determine the full extent of the unauthorized access attempts. During the investigation, URE determined that the vendor-provided custodial employee had also entered the control center PSP, without a valid access card. Personnel within the PSP allowed the individual inside after the individual requested access locally after his or her attempt to use the access badge failed. URE did not record and maintain manual logs of this individual's physical access since the individual was not properly escorted in the PSP in accordance with the established visitor control program.

URE had a physical security program established for addressing all CIP physical security measures. The program applies to all URE facilities and personnel and requires all URE facilities containing assets subject the CIP Reliability Standards to document a physical security plan. Additionally, URE's program requires continuous escorting of any individual without authorized unescorted physical access to a PSP,

including specific logging of the visitor's name, date, and time of entry and exits. URE also had procedures requiring it to log and monitor access to PSPs 24 hours per day, seven days per week.

SERC determined that because URE did not record or maintain logs of a vendor employee's physical access, URE did not record sufficient information to identify uniquely the individual and the individual's time of access to the URE PSP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be when the vendor employee gained access to the PSP without creating a manual log entry following a biometric mismatch and URE security personnel confiscated the badge with which the vendor employee was attempting unauthorized access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The vendor employee had undergone URE's cyber security awareness training prior to accessing the PSP. URE had a biometric reader in place at the access point to the PSP that alarmed when the vendor employee attempted access with an incorrect badge. Additionally, following the biometric mismatch, URE's security personnel acted swiftly to confiscate the badge used during the access attempt. The PSP that the vendor employee entered was a control center manned and monitored 24 hours a day, seven days a week.

CIP-007

The purpose statement of Reliability Standard CIP-007 provides in pertinent part:

> Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009.

CIP-007-1 R1 (SERC201000678)[20]

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

[20] URE's violation applies from Version 1 through Version 2 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

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 was in violation of CIP-007-1 R1. URE reported that its procedures ensured functional testing for significant changes to systems, but the associated testing did not include an assessment of cyber security controls.

URE's documented change management program, which was applicable to all CCAs and Cyber Assets located inside the ESPs, required testing of significant changes to all existing and new Cyber Assets located inside an ESP. URE revised the program to include CIP-007 R1 testing of significant changes to existing and new Cyber Assets. Upon these revisions, URE's processes and procedures required the testing of significant changes to existing Cyber Assets within the ESP to ensure that they do not adversely affect existing cyber security controls. URE's actual performance of testing cyber security controls was contingent on the installation of certain software, and URE did not implement this software until approximately 22 months after URE revised the program.

As a result, SERC determined that URE failed to test security controls for 142 CCAs (including workstations, servers, modems, switches, and routers) and 69 Cyber Assets located inside an ESP (including printers, workstations, servers, modems, and tape libraries) until URE implemented the software.

SERC determined that URE was in violation of CIP-007-1 R1 for failing to test significant changes to new and existing Cyber Assets within the ESP to ensure that they do not adversely affect existing cyber security controls. While URE did have policies and procedures in place that enforced testing of both

functional and security controls, it failed to test significant changes for adverse effects on existing security controls.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through when URE implemented software to enable it to test cyber security controls for CCAs and Cyber Assets.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to test cyber security controls prior to implementation in the production environment for an extended period could have introduced security vulnerabilities to critical and non-critical Cyber Assets located inside the ESP. URE did have some protections in place. URE had procedures in place for change control and testing of significant changes. URE did complete functional testing prior to implementation in the production environment, which reduced the risk of operational downtime. The ESPs, where the devices resided, utilized real-time monitoring, which included IDS.

CIP-007-1 R2 (SERC201000734)

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.

SERC conducted a compliance Spot Check of URE. In the audit detail letter, SERC notified URE that CIP-007-1 R2 would be in scope of the scheduled Spot Check.

The CIP Spot Check team reported a violation of CIP-007-1 R2 because URE did not document the required ports and services for the sampled Cyber Assets within the ESP, and did not disable ports and services that were not required for normal or emergency operations.

SERC reviewed the results of the URE cyber vulnerability assessment (CVA) and determined that URE did not provide a baseline list for all required ports and services. The CVA showed that multiple open ports lacked justification for being open. Additionally, specific ports and services on control center devices were enabled but not required for normal and emergency operations. URE completed a full-scope assessment of the issue and found no baseline documentation for 211 devices (CCAs and non-CCAs). URE attested to 174 of those devices having ports and services enabled that were not needed for normal or emergency operations.

SERC determined that URE failed to enable only those ports and services required for normal and emergency operations. Specifically, URE did not provide evidence to support having enabled ports and services on all Cyber Assets, resulting in a violation of CIP-007-1 R2.

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

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Failure to ensure that only ports and services needed for normal and emergency operations were enabled could allow unauthorized individuals or malware to exploit these ports, and thereby disrupt operations or gain unauthorized access to CCAs. URE has two violations included in this Settlement Agreement that contributed to the serious or substantial risk. The first violation was for URE's failure to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls (SERC201000678) on all CCAs and non-CCAs. The second violation was URE's failure to ensure that, at all access points to the ESP, only ports and services required for emergency operations and for monitoring Cyber Assets within ESPs were enabled (SERC201000730). URE did have some protections in place. URE had IDS devices in place inside the ESP and on the corporate network. URE used an access control model that denied access by default. URE had a third party performing security logging and monitoring. Finally, URE had processes and procedures in an attempt to ensure the proper management of ports and services on Cyber Assets located inside the ESP.

CIP-007-1 R3 (SERC201000735)[21]

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.

SERC conducted a compliance Spot Check of URE.

URE's cyber security patch and vulnerability management program applies to all URE functions and all Critical and non-critical Cyber Assets within URE's ESP. Although URE reviewed this program annually, URE relied on procedural documents to provide the details of its security patch management program.

SERC reviewed one of URE's procedures, the URE control system procedure put in place to implement the URE cyber security patch and vulnerability management program. SERC determined that this procedure did not address the evaluation of patches within 30 calendar days of availability, testing of patches, and deployment of patches to several device types, as required by CIP-007-1 R3.1.

Additionally, SERC reviewed the URE patch evaluation list for some of URE's functions, provided during the Spot Check as evidence of URE's implementation of the procedures described above. This list

[21] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement changed from Version 1 to Version 2. The language of the Requirement remained the same from Version 2 to version 3. Version 2 removed the following words from R3.2: "…or an acceptance of risk."

showed multiple security patches released without a completed assessment or a documented mandatory installation date. The list did not include information regarding the patches' applicability or compensatory measures applied to mitigate risks in the event that a patch was not applied. The patch evaluation list showed evidence of the assessment of security patches for operating systems but did not show evidence of URE's assessment of security patches applicable to non-operating system software.

Finally, to evaluate URE's security patch management program for other functions, SERC reviewed URE's CVA, which indicated that URE failed to assess certain historical security patches applicable to Cyber Assets inside of an ESP and failed to apply them as necessary. The CVA results also indicated that URE failed to maintain documentation of security patch assessments and the associated software inventory required to support patch review as required by CIP-007-1 R3.2.

SERC determined that URE was in violation of CIP-007 R3 because it failed to provide evidence of an established security patch management program for evaluating and installing applicable cyber security software patches for all Cyber Assets within its ESPs.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to assess and install security patches could have resulted in unaddressed vulnerabilities for extended periods, increasing the risk of a successful intrusion. URE did have protections in place to mitigate the potential risk. The unassessed security patches were applicable to a limited number of non-critical Cyber Assets. All of URE's Cyber Assets resided within ESPs and PSPs. Access to Cyber Assets within the ESP from outside the ESP required two-factor authentication. During the violation period, URE's electronic access and control monitoring devices did not identify any malicious activity affecting the involved Cyber Assets.

CIP-007-3a R3 (SERC2012010883)

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

URE submitted a Self-Report stating that it was in violation of CIP-007-3 R3 because URE failed to assess three operating system vendor advisories for applicability within 30 days of availability.

The three advisories identified in URE's Self-Report were applicable to devices with a specific operating system, limiting the issue to approximately 20 non-critical Cyber Assets out of 140 contained in the

associated ESP. The vendor-assigned vulnerability rating for these advisories was "High." The security patches associated with these advisories became available but URE did not assess them until approximately six months later, and did not document the assessment until approximately eleven months after the security patches became available. URE installed the three security patches approximately five months after URE documented the assessment. URE only installs assessed security patches during scheduled system outages, which typically occur twice a year. In this instance, URE failed to train adequately the administrator responsible for assessing these patches on the manual process for security patch assessment.

SERC determined that URE failed to document the assessment of security patches and security upgrades for applicability within 30 calendar days of availability and failed to document the implementation of such security patches.

SERC determined the duration of the violation to be from when the first security patch was available through when URE assessed the missing patches.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The security patches missed were applicable to a limited number of non-critical Cyber Assets. All of URE's Cyber Assets resided within ESPs and PSPs. Access to Cyber Assets from outside the ESP required two-factor authentication. URE's EACM devices did not identify any malicious activity during the violation period that would have affected the 20 non-critical Cyber Assets at issue.

CIP-007-1 R4 (SERC201000566)[22]

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

[22] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version.

compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

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

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R4. URE identified a single server located inside the ESP that did not have anti-malware software installed. According to URE, the server did not support anti-malware software due to hardware resource restrictions. URE used the server for archiving historical data, and the server had no ability to control elements of the BPS.

URE's CIP-007 R4 anti-malware process in place at the time of the Self-Report addressed CIP-007 R4 and included a requirement to file a TFE in cases where URE could not install anti-malware. URE failed to submit a TFE for this server. This violation resulted from URE's failure to follow its established process.

SERC determined that URE was in violation of CIP-007 R4 because it failed to install malware and anti-virus protection tools or implement and document compensating measures on the identified device.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until 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 server at issue was located inside a PSP and ESP and had no ability to control elements of the BPS. The other devices in the ESP had anti-malware software installed, which should have restricted the spread of malware in the unlikely event that the device became infected.

CIP-007-1 R4:4.2 (SERC201000736)[23]

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

SERC conducted a compliance Spot Check of URE.

[23] URE's violation applies from Version 1 through Version 3 of the Standard since the duration spans the enforceable dates of each version. The language of the Requirement remained the same in each version. However, beginning with Version 2, the phrase "or an acceptance of risk" no longer appeared in Requirement R4.1.

The CIP Spot Check team reported a violation of CIP-007-1 R4.2 because URE did not have a process for testing and installing antivirus and anti-malware "signatures" for all Cyber Assets.

URE first implemented a procedure for testing antivirus and malware prevention tools nearly six months after the date on which URE was required to comply with CIP-007-1 R4. This procedure addressed the antivirus and prevention tools used to address compliance with CIP-007 R4. This procedure required each URE strategic business unit (SBU) to create a process for the testing and installing of antivirus and malware signatures. However, URE failed to provide SBU processes for testing antivirus and malware prevention signatures.

URE also provided evidence of pattern testing conducted by the vendor to minimize adverse effects during the deployment of antivirus and malware signatures to that vendor's products. The evidence also described the vendor's antivirus definition certification process for verifying and validating signatures. SERC determined the vendor's performance of testing did not eliminate the need for URE do so.

SERC determined that URE violated CIP-007 R4.2 because it failed to document a process for the testing of antivirus and malware prevention signatures.

SERC determined the duration of the violation to be from when 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 did use antivirus software and other malware prevention tools on Cyber Assets located inside of the ESP, where technically feasible, excluding the device involved in the instant violation of CIP-007-1 R4 (SERC201000566). URE attested that it tested antivirus and malware signatures, prior to installation, on a development system that reflected the production system. URE did provide evidence of vendor testing of antivirus and malware prevention signatures prior to deployment.

CIP-007-1 R5 (SERC201000570)

CIP-007-1 R5 provides:

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

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

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

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

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

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

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

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

R5.2.3. Where such accounts must be shared, the Responsible Entity shall have a policy for managing the use of such accounts that limits access to only those with authorization, an audit trail of the account use (automated or manual), and steps for securing the account in the event of personnel changes (for example, change in assignment or termination).

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

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

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

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

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

URE submitted a Self-Report, stating that it was in violation of CIP-007-1 R5.2 because it failed to remove or disable 48 accounts. The 48 accounts in question existed on servers and workstations with various operating systems prior to the mandatory date of compliance. URE identified all of the account issues in an annual account review, which included all local accounts on all Cyber Assets located inside of an ESP. Some of the operating systems were equipped with controls to disable automatically accounts with 90 days of inactivity, resulting in all those accounts being disabled but not removed or deleted. The other operating systems were equipped with no such controls. URE removed all these accounts on the same day it submitted the Self-Report.

While SERC staff was performing its assessment and determining the scope of the violation, the following additional issues were reported:

1. During a CIP Spot Check, SERC made the following determinations:

    a. URE failed to remove, disable, rename, or change passwords for default accounts for three Cyber Assets prior to putting them into service. Additionally, URE did not require and use passwords for all accounts on all of its Cyber Assets within the ESPs. Lastly, URE did not change passwords annually for all accounts on Cyber Assets within the ESP.

    b. In at least one instance, a default password on an account existed prior to the mandatory date of compliance and had not been changed. Additionally, URE's CVA identified three systems that had default accounts with unchanged passwords. The CVA also identified systems with accounts no longer needed, including a Cyber Asset with a password that had not been changed since the mandatory date of compliance. The devices in question were servers and workstations that were capable of enforcing the password requirements of CIP-007 R5.3 and Ethernet modems that are infrequently logged into and not capable of enforcing the password requirements of CIP-007 R5.3.

c. URE had four administrative accounts with passwords older than one year because URE failed to change these passwords annually, as required. The passwords for the accounts were late by: 1) 135 days for account one; 2) 17 days for account two; 3) 7 days for account three; and 4) 48 days for account four.

2. URE submitted a Self-Report to SERC stating that 16 servers (14 CCAs and 2 non-critical Cyber Assets) were not configured to enforce the password requirements of CIP-007 R5.3. Although the servers were capable of enforcing the password requirements of CIP-007 R5, URE did not discover the failure to configure the passwords until 19 months after the mandatory date of compliance. As a result, SERC determined that URE failed to ensure that all Cyber Assets within its ESPs had passwords meeting the parameters of CIP-007 R5.3.

3. URE submitted a Self-Report to SERC stating that while performing its annual CVA as required by CIP-007 R8, it discovered non-compliant configuration files on a backup server. Specifically URE found that controls for technically enforcing the use of a special character were not in place. More specifically, the configuration option which specifies the minimum number of special characters required, was not enabled, allowing users to select a password that did not have a special character, as required by CIP-007 R5.3.2.

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

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to remove default accounts or change passwords on default accounts could have left Cyber Assets vulnerable to compromise since many default account credentials are public information. Failing to change passwords on an annual basis and failing to use strong password controls could leave passwords, and the systems they protect, susceptible to attacks potentially allowing an unauthorized user to access or compromise a system. URE did have protections in place to mitigate the potential risk. All devices were located in an ESP and PSP. URE's Cyber Assets reside behind firewalls and physically secured facilities with card readers and biometrics controls. The ESPs where the devices resided utilized real-time monitoring, including IDS that monitored the switch ports connected to the devices. Malware prevention and other security controls, such as patching, local firewalls, and antivirus software, remained operational and up-to-date for the period in question.

CIP-007-1 R6 (SERC201000567)

CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
> >
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
> >
> > R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
> >
> > R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

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

URE submitted a Self-Report to SERC stating that it had a violation of CIP-007-1 R6. URE identified three Cyber Assets located inside an ESP that were not logging security events due to improper configurations and technical infeasibility. Two of the devices were servers that did not have the security logging software installed and configured properly.

The third device was an antiquated server used for the archiving of historical data and had no ability to control elements of the BPS. This device did not support the security logging client used by URE. Despite this, URE failed to file a TFE for the device. This server was in place prior to the mandatory date of compliance and was removed from operation approximately fifteen months after the mandatory date of compliance.

While SERC was performing its assessment and determining the scope of the violation, URE reported the following additional issues:

1. URE reported that it failed to configure some hosts to send security monitoring messages and to log such messages, as required. Specifically, URE failed to configure 12 out of 215 devices in an established ESP to send logs to the centralized server. In some cases, the security logging software was not installed and configured properly, and in others the centralized sever was not configured to receive logging data. SERC determined that URE failed to ensure that all Cyber Assets within the ESPs, as technically feasible, implement automated tools or organizational process controls to monitor system events related to cyber security.

2. URE reported that the centralized server was not processing cyber security logs for seven non-critical Cyber Assets. The systems were configured to log events locally and to send the logs to the server. The server was not configured properly to receive or monitor log events from the seven assets. URE discovered this issue during its annual review of the security monitoring controls. The improper configuration dated back to the earliest in-service date of the seven devices, and URE corrected the configuration approximately two years later.

3. URE reported that during two network upgrades, security logging and monitoring was unavailable for some critical and non-critical Cyber Assets. On two occasions, URE experienced a network outage that resulted in a failure of logging and monitoring for seven Cyber Assets. The two network outages resulted from the need to upgrade software for some URE network devices for both security and functional purposes. These network devices managed the connection of the seven Cyber Assets in question to the central logging server. During the two network upgrades, logging and monitoring was unavailable for a total of 120 minutes.

    a. The first outage lasted 30 minutes. Three Cyber Assets did not have complete redundancy and were not capable of storing logs locally for this period, resulting in a disruption in logging and monitoring for the three assets at issue.

    b. The second outage occurred approximately five months after the first outage and lasted 90 minutes. Four Cyber Assets were not sending logs to the centralized server and were unable to archive logs locally for the outage period, thus resulting in a disruption in logging and monitoring for the four devices at issue.

SERC determined that URE was in violation of CIP-007 R6 for failing to ensure that all Cyber Assets within the ESP implement automated tools or organizational process controls to monitor system events related to cyber security.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE until 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 monitor system events related to cyber security for its Cyber Assets within the ESPs could have resulted in a security breach going undetected. An undetected security breach may have rendered CCAs inoperable, resulting in the loss of monitoring and control of the BPS. URE's failure to retain logs related to security events could have impaired its ability to conduct an incident response. URE did have protections in place to mitigate the potential risk. The ESPs where the devices resided utilized real-time monitoring, which included IDS that monitored the switch ports connected to the devices. Malware prevention and other security controls remained operational and up-to-date for the period in question. Instances involving network outages were controlled events with trained technical personnel present for the entire duration of the outages and actively monitoring the system conditions. URE reviewed all firewall logs and found no unauthorized access or access attempts.

CIP-007-3a R8 (SERC2012011013)

CIP-007-3a R8 provides:

> 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:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> R8.2. A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;
>
> R8.3. A review of controls for default accounts; and,
>
> 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-007-3a R8 has a "Lower" VRF and a "Severe" VSL.

SERC conducted a compliance Spot Check of URE.

During the Audit, SERC determined that URE had violated CIP-007-3a R8.2 and R8.3 because URE did not perform a CVA of all Cyber Assets within the ESP at least annually, as required. Specifically, URE had excluded network switches and routers from aspects of its CVA.

URE performed CVAs for devices, however, URE's evidence did not demonstrate the review of all enabled ports and services on network routers and network switches within the ESP as required by CIP-007-3 R8.2.

Additionally, URE did not fully perform a review of controls for default accounts on switches and routers within the ESP as required by CIP-007-3 R8.3. URE stated that it used the same default account reviews as performed for Electronic Access Points (EAPs), pursuant to CIP-005-3 R4.4. However, the scripts provided for the EAPs had been hard coded with account names specific to the firewalls. Therefore, these scripts were inadequate for discovering default accounts on the network switches and stand-alone routers.

SERC determined that URE was in violation of CIP-007-3a R8.2 and R8.3 because it did not perform a CVA for all Cyber Assets within the ESP. Specifically, URE did not demonstrate that it reviewed ports and services required for operations, or review controls for default accounts for all Cyber Assets within the ESP.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE until 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. Despite URE's inability to substantiate a review of ports and services enabled on network switches and routers residing inside the ESP, the switch configurations make the ports and services incapable of logical port filtering. URE performed a complete CVA of all electronic access points, ensuring that its ESP's perimeter defenses were properly hardened. While URE did not perform a review of controls for default accounts on the network switches and routing devices residing inside the ESP, a malicious attacker attempting to exploit said devices would have had to cross the electronic access point firewall perimeter defenses first. URE maintains a contract with a third-party security vendor that provides security analysis and prevention services at all times. The security vendor has monitoring devices to assist in real-time monitoring of the URE ESP and constantly monitors the URE network for malicious activity. The vendor's monitoring also includes immediate notification of detected security anomalies.

Regional Entity's Basis for Penalty

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

1. URE self-reported 17 of the violations, which SERC considered a mitigating factor;
2. URE was cooperative throughout the compliance enforcement process, which SERC considered a mitigating factor;
3. URE had an internal compliance program (ICP) at the time the violations occurred, which SERC considered a mitigating factor;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. the violations of CIP-007-1 R1 and R2 (SERC201000678 and SERC201000734) posed a serious or substantial risk to the reliability of the BPS, as discussed above;
6. in addition to paying the monetary penalty, URE agreed to:
    a. Implement certain physical security measures beyond those required to comply with the applicable NERC Reliability Standards. URE installed revolving doors designed to prevent tailgating at the outermost entry points at the facility housing its control center, a data center, and its security-monitoring center. URE also installed high-resolution surveillance cameras to enable earlier detection of events and enhanced forensic work after an event. URE implemented biometric identity authentication tools; and
    b. Implement a training and awareness program that exceeds the requirements of the applicable NERC Reliability Standards. This program includes a professionally developed computer-based interactive training that is required of all employees, not just those with access to CCAs. URE ensures awareness of security issues through regular communications, posters, tips, and alerts.
7. 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 two hundred fifty thousand dollars ($250,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[24]

CIP-002-2 R2 (SERC201000685)

URE's Mitigation Plan to address its violation of CIP-002-2 R2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005822-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the scoping workshop checklist to address new construction and modifications at existing Critical Asset facilities;
2. revise the risk-based assessment methodology to require reissuance of the Critical Asset list after the commissioning of new Critical Assets; and
3. update the Critical Asset list.

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

1. the newly revised and updated scoping workshop checklist;
2. the new RBAM procedure; and
3. a copy of the Critical Asset list update letter.

CIP-004-1 R3 (SERC201000568)

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005271-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove physical access;
2. implement a process to include at least two reviewers during quarterly reviews; and

[24] *See* 18 C.F.R § 39.7(d)(6).

3. implement a process to conduct daily reviews of physical access changes to PSPs.

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

1. the request to remove the individual from the access system;
2. confirmation of removal completed; and
3. evidence of the establishment of the daily review process showing the reoccurrence of the monthly review process and examples of the daily report.

CIP-004-1 R4 (SERC201000569)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005273-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove accesses and documented changes as required;
2. review local and centralized accounts during the quarterly review;
3. implement detection reporting process to detect and report configuration changes to ensure no local accounts are added without authorization and all account changes are documented using the business unit's change management process and reviewed and approved by the change control board prior to being executed;
4. formalize procedural steps for documenting physical access changes;
5. implement a daily review of the human resources system change report, which identifies job changes and organizational changes for personnel across the entire entity and updates the master list as needed on a daily basis;
6. implement a process for IT security to review the daily human resources termination review report for any changes affecting access lists and forward such information to the appropriate business unit; and
7. train access control employees and took steps to ensure awareness of regulatory timelines for access removals and documentation of access removals.

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

1. change request to remove cyber access for the individual in question;
2. quarterly review notice;
3. training roster for access control personnel;
4. checkout procedure explanation communicated to targeted personnel;
5. HR termination report;
6. add/remove report;
7. job change report;
8. employee checkout procedure;
9. access control procedure; and
10. Configuration change monitoring report example.

CIP-004-3 R4 (SERC2012010884)

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 is designated as SERCMIT008635 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. execute an intergroup agreement allowing senior executives to be granted access to CCAs, provided that such individuals meet the PRA and training requirements; and
2. notify authorized individual that access to this PSP had been granted to the involved individuals pursuant to this intergroup agreement.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a copy of the intergroup agreement.

CIP-005-1 R1; R1.5 (SERC201000729)

URE's Mitigation Plan to address its violation of CIP-005-1 R1; R1.5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is

designated as SERCMIT010429 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. gather functional requirements for a new, locally managed, Security and Event Management (SIEM) system;
2. complete the project scope development and detailed project plan for the new SIEM system implementation;
3. review the SIEM devices to ensure that new devices provide full coverage leaving no gaps in the monitoring system;
4. determine EACM device placement;
5. install all new hardware to ensure that new SIEM system is ready for testing;
6. conduct testing to ensure full functionality of new SIEM system; and
7. complete installation of new SIEM system and provide any necessary training.

CIP-005-1 R1 (SERC2012011010)

URE's Mitigation Plan to address its violation of CIP-005-1 R1was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010430 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. meet with project manager (PM) to verify schedule;
2. implement Phase I of network and installation of infrastructure;
3. run Phase I systems in parallel for testing;
4. complete Phase I network cut-over;
5. meet with PM to verify schedule for Phase II;
6. implement Phase II of network and installation of infrastructure;
7. complete Phase II network cut-over;
8. eliminate SPAN ports through network re-architecture project;

9. review Project Scope for completion;
10. transition CIP-005 governance to comply with controls provided in CIP 005-5 and adoption of revised definitions for "Electronic Access Point," "External Routable Connectivity," and "Electronic Security Perimeter;" and
11. review ESP diagrams and revise to align with CIP-005-5 governance.

CIP-005-1 R2; R2.2 (SERC201000730)

URE's Mitigation Plan to address its violation of CIP-005-1 R2; R2.2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010422 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the rule at issue to restrict inbound network access;
2. remove VPN access through the facility's firewall; and
3. ensure that firewall configurations would be reviewed annually in the annual CVAs.

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

1. a change ticket as evidence of the configuration change to remove the rule at issue to restrict inbound access;
2. an email from the subject matter expert attesting to the fact that VEPN access was removed; and
3. a CVA procedure which specifies that a review of ports and services at access points is reviewed as part of the CVA.

CIP-005-1 R3; R3.2 (SERC2012011011)

URE's Mitigation Plan to address its violation of CIP-005-1 R3; R3.2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010424 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace and configured new firewalls to generate adequate logs;
2. update all related network drawings, ESP drawings, and asset inventories to reflect the firewall replacements;
3. update CVA procedures to ensure that a CVA is conducted to review firewall configurations.

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

1. two screenshots showing that the new firewalls that could robustly handle the logging requirements were logging;
2. updated network drawings, ESP drawings, and asset inventories; and
3. an updated CVA procedure that addresses the annual review of electronic access points.

CIP-006-1 R1.1 (SERC201000682)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005283-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform an assessment of the current locations of each access control system communication lines between PSPs at its facilities;
2. continue with cutover project. This will move control system components and communications from the corporate network to a URE control system network, further isolating the control system;
3. verify that the unprotected routable network cables outside a PSP will be protected by running it through steel conduit; and
4. file a TFE and implement compensating measures as stated above. The primary first line of protection is the steel conduit enclosures that protect the communication networks. These are also contained in an area of the plant that has very limited access with other physical protections in place.

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

1. independent third-party assessment of the facilities in question;
2. schedule review of network changes and cutover schedule;
3. mitigation schedule;
4. copy of work order necessary for conduit enclosure completion; and
5. photo of the type of conduit enclosing the cables in two facilities.

CIP-006-1 R1 (SERC201000731)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010393 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. secure the hole in the wall to less than a 96 square inch opening by securing a steel bar horizontally across the opening; and
2. update the PSP drawings in the physical security plan to reflect the proper PSP perimeter was completed.

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 the opening was closed with horizontal bars that reduced the opening to less than 96 square inches; and
2. an edited version of the PSP drawing for the area in question.

CIP-006-1 R1 (SERC2012010586)

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007759-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct physical security walk-downs at all Critical Assets to ensure that all access points have the appropriate security measures in place to control access to the PSPs; and
2. secure operable windows to render them inoperable or smaller than 96 square inches.

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

1. photos showing riveting shut of the operable windows to the fixed frames in the PSP in question and a statement noting completion; and
2. photos showing screening of the operable windows and an email statement noting completion.

CIP-006-1 R1; R1.8 (SERC2012010860)

URE's Mitigation Plan to address its violation of CIP-006-1 R1; R1.8 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008652-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove access to the PACS;
2. establish and populate a new active directory security group for administrators that requires an individual to have a valid PRA prior to being added to the directory;
3. change the system control and account passwords;
4. stop and disabled unnecessary ports and services;
5. uninstall software associated with unnecessary services during approved outage window; and
6. update the disaster recovery test plan, execute test plan, and schedule the next disaster recovery test plan.

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

1. properties shown for creating a new group with proper PRAs and written explanation of emails previously submitted;

2. IT tickets showing the disabling of ports and services identified during pre-audit review as no longer required for system operation;
3. disaster recovery plan showing an updated recovery test plan;
4. four additional emails showing scheduled reviews; and
5. work-request documentation for "password reset."

CIP-006-3c R1; R1.6.1 (SERC2013012360)

URE's Mitigation Plan to address its violation of CIP-006-3c R1; R1.6.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009616 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke the contractor's access to the PSP at issue;
2. retrain the contractor on the facility's visitor management policy;
3. issue a security awareness bulletin on the existing visitor management policy to all personnel with unescorted access to the PSP at issue; and
4. review the existing visitor management policy with all employees with unescorted access to the PSP at issue.

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

1. a training roster showing the contractor retraining was complete; and
2. a copy of a security awareness bulletin that was distributed to all personnel within the business unit.

CIP-006-2 R3 (SERC201000679)

URE's Mitigation Plan to address its violation of CIP-006-2 R3 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005290-1 and was submitted as non-public information to in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. relocate the firewall at issue into a defined PSP; and
2. modify the design change notice procedures to include a security review of all hardware additions and modifications, thereby preventing future access control devices from not being located in a PSP.

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

1. firewall compliance report (before and after)
2. work order detailing work and completion;
3. system test plan to verify operability after completion; and
4. revision that illustrates cyber security checkpoint when making system changes.

CIP-006-2 R3 (SERC201000733)

URE's Mitigation Plan to address its violation of CIP-006-2 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010428 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete conceptual design for the project and determine necessary resources to complete the project;
2. develop preliminary physical protection specifications required for the physical space selected;
3. review completed physical design details during an on-site meeting and walk down and review all final design drawings (physical) and final project specifications;
4. review physical engineering design changes and determine any environmental effects;
5. start necessary field construction work;
6. verify construction progress has reached the scheduled halfway point;
7. perform acceptance testing to ensure the installation is functional, complies with design specifications, and is within scoping requirements;
8. document functional testing; and

9. close all outstanding work orders associated with the project.

CIP-006-1 R4 (SERC2012010585)

URE's Mitigation Plan to address its violation of CIP-006-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007760-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install card readers and alarm contacts on equipment lift vestibule double doors to provide for logging and monitoring of PSP access point; and
2. modify physical security plan to redefine PSP to remove equipment lift as an access point and identify vestibule double doors as a new access point.

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

1. card reader access request and reader access system test; and
2. security plan with updated PSP drawing.

CIP-006-3a R4 (SERC201000683)

URE's Mitigation Plan to address its violation of CIP-006-3a R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007581 and was submitted as non-public information to in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. modify the configuration of the access point to the PSP at issue to ensure that doors would remain locked during fire drills;
2. modify alarm response procedures to require physical verification of functionality of locks prior to clearing alarm;
3. add check of functionality of physical access control systems to post-fire drill procedures; and
4. train building security personnel on required steps after a fire drill.

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

1. documentation of verification that doors remain secure during fire alarm testing;
2. Email with new alarm verification process explained in detail;
3. Copy of building emergency response plan for the area in question showing instructions for security personnel to verify doors remain secure; and
4. Training roster and training materials.

CIP-006-3c R6 (SERC2012009109)

URE's Mitigation Plan to address its violation of CIP-006-3c R6 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT006623-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. confiscate the badge and revoke access for vendor-provided custodial personnel at the facility in question;
2. conduct an internal investigation;
3. issue interim process for granting access outside normal business hours;
4. transition cleaning services to internal personnel;
5. review and update procedures for granting access to PSPs outside normal business hours; and
6. retrain individuals responsible for managing and controlling access to PSPs.

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

1. access group "action history" for revoking access for the vendor provided custodial personnel;
2. documentation of internal investigation by URE personnel;
3. copy of interim process for operation center access after normal business hours and copy of email transmittals;
4. emails documenting transitioning to URE personnel for cleaning of the operating center;

5. training roster documenting retraining of operating center personnel on revised criteria and processes; and
6. copy of updated revised criteria for granting access after normal hours.

CIP-007-1 R1 (SERC201000678)

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005279-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create and implement a technical procedure requiring the necessary testing; and
2. install an operating system to monitor for changes to security controls in ESPs.

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

1. Cyber Asset Test Plan along with evidence of review;
2. change tickets requesting authorization and implementation of a security and data integrity tool used for monitoring and alerting on specific file change(s) on a range of systems;
3. evidence of the data tool contract;
4. evidence of the data tool network modifications;
5. work order for hardware associated with the data tool implementation;
6. change ticket for solution testing and production rollout evidence;
7. project completion and closeout documentation; and
8. copy of testing process in place.

CIP-007-1 R2 (SERC201000734)

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010426 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a technical practice document providing guidance when significant changes and security changes are performed;
2. implement a data tool to detect changes to Cyber Assets for security, document, and store all approved ports and services within the data tool;
3. implement a script to detect authorized/unauthorized ports detection in the data tool and alert support personnel of any changes, implement command on Cyber Assets for port number, port name, and executable, and verify the information in the file for approved ports and services;
4. add additional technical practice governance in business unit's procedure, Cyber Asset test plan, regarding evaluation for ports and services;
5. verify vendor or entity documentation that specific port or service is required for normal and emergency operations and disable; and
6. project closeout and implement annual reviews as part of the CVA to prevent future recurrence.

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 Asset test plan procedure document;
2. a copy of change ticket detailing the data tool project;
3. an excerpt from SCADA workstation ports list;
4. a copy of change ticket detailing implementation of the script;
5. a copy of change ticket detailing activities for implementation of commands on Critical Asset devices for port name, and executable and verify;
6. a technical practice document showing additions to the document in the title page and revision log;
7. a copy of the revision log for a procedure showing addition to the procedure plus an example of change control documentation when action is required; and
8. a procedure revision log showing additions and change ticket closed.

CIP-007-1 R3 (SERC201000735)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010423 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. eliminate legacy assets and remove difficult-to-patch legacy servers from ESP;
2. revise the patch management program and update procedure addressing enhancements to security patch evaluation and rating process to facilitate compliance;
3. revise hydro operations and facility's procedures to align with URE patch management program;
4. deploy updated procedures to those involved with the patch management program;
5. assess missing patches by reviewing vulnerability scan reports on relevant assets;
6. obtain relevant patches from proper sources and perform security testing covering each patch before deployment to production assets; and
7. coordinate outages with plant/facility management to schedule appropriate times for asset outages and install patches on production assets, pending successful security testing.

CIP-007-3a R3 (SERC2012010883)

URE's Mitigation Plan to address its violation of CIP-007-3a R3 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008191-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a formal work instruction to address adding new administrators; and
2. apply the missed security patches missed to the applicable Cyber Assets.

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

1. formal work instruction; and
2. screen shots illustrating application of the three security patches.

CIP-007-1 R4 (SERC201000566)

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005276 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace the existing server hardware and completed all necessary configurations enabling the new server to run malware prevention tools, as required;
2. configure the application to replace the archive server and cluster configuration to provide failover support;
3. install management tools once the operating system and cluster software was configured;
4. configure the system with the IP and hostname resources from the archive server to facilitate minimal downtime; and
5. power off and remove from network the old archive server once the cutover was complete.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the appropriate change request and change tickets from the change management process.

CIP-007-1 R4; R4.2 (SERC201000736)

URE's Mitigation Plan to address its violation of CIP-007-1 R4; R4.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010421 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform project scoping;

2. develop implementation schedule for testing malware signature files;
3. configure solution for testing malware signature files;
4. complete implementation of testing process;
5. develop work instruction or procedure detailing testing of malware signature files; and
6. train applicable staff on the testing process.

CIP-007-1 R5 (SERC201000570)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC stating that it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005274-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove local accounts;
2. modify the quarterly review process to include review of local accounts in addition to centralized accounts;
3. implement quarterly reviews of accounts including at least two reviewers;
4. implement a monitoring and reporting system to report configuration changes;
5. document all account changes relating to personnel with access to CCAs using the change management process;
6. change passwords for default accounts as required;
7. configure monitoring system to generate a daily password age report and alert personnel of passwords older than 300 days and implement other technical controls to ensure passwords are changed;
8. implement a system integrity monitoring solution to monitor assets to verify the integrity of cyber security posture;
9. research potential pluggable authentication module configurations with support of system vendors;
10. test the solution per change management process;
11. rollout the production of the solution per change management process;

12. document the solution per the change management process;
13. create automated alerts on passwords that are older than 330 days with the data tool reports;
14. issue a change request ticket to change passwords when it is older than 330 days;
15. create electronic calendar notification alert when a password reaches 330 days for Cyber Assets that do not report to automated monitoring and alerting system;
16. review and discuss details of violations and mitigation plan with staff; and
17. configure password requirements and monitoring tools to ensure complexity parameters are implemented as required.

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

1. change tickets for changing passwords, account removal, and the disabling of accounts;
2. spreadsheets denoting accounts;
3. emails showing evidence of removal;
4. quarterly review notice and documentation;
5. documentation showing the data tool implementation;
6. change ticket for password changes of default accounts;
7. work orders for password changes;
8. the data tool report to configure system integrity monitoring solution to monitor asset;
9. example documentation of hardware listing in data request;
10. work order for hardware changes;
11. the data tool report showing system integrity monitoring;
12. change ticket dealing activities to implement a system integrity monitoring solution
13. research of configurations;
14. documentation of solution test per change management requirements;
15. change ticket showing production rollout of solution;
16. document showing project completion;
17. documentation of project closeout from change ticket;

18. change order creating automated alerts on aging passwords;
19. email verifying automatic notification for password resets;
20. documentation showing electronic calendar notification;
21. documentation showing staff review and discussions on the details of the violation and mitigation plan;
22. work order documenting password change;
23. change order and work order detailing changes to the password enforcement parameters configuration; and
24. documentation illustrating enforcement of password complexity requirements.

CIP-007-1 R6 (SERC201000567)

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005280-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Issue 1:
    - expand security event log files on the two assets to support compliance with the standard and configure the log files to be automatically archived on a weekly basis so that log data is retained;
    - replace existing server hardware with new hardware and all associated network, storage, and application installation;
    - configure the application to replace the archive server and cluster configuration to provide failover support; and
    - configure the system, cutover to the new system, and retire the old archive server and remove it from the network.
2. Issue 2:
    - research configuration options permitting strict compliance;
    - determine preferred technical solutions;

- test solutions per its change management process;
- deploy software and system modifications as needed; and
- implement the preferred technical solutions.

3. Issue 3: configure its servers to accept and monitor logs from affected Cyber Assets.
4. Issue 4: install an alternate log archive storage system in the event of a primary network monitoring outage, preventing loss of logs during outages.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted the appropriate system change request and change tickets from the change management process, showing any associated procedural modifications.

CIP-007-3a R8 (SERC2012011013)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010268 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. append existing CVA to document reviews required by CIP-007-3 R8.2 and R8.3 for each Cyber Asset within the ESP; and
2. create work papers to substantiate required reviews for ports and services and default accounts for network switches and routers within the ESP.

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

1. revised CVA procedure document showing the addition of the execution status of CIP-007 R8.2 and R8.3 for each asset in the ESP; and
2. four files demonstrating the creation of work papers to document the CIP-007 R8.2 ports and services and R8.3 default account review for network switches and routers within the ESP.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[25]
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,[26] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on April 15, 2014. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a two hundred fifty thousand dollar ($250,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE self-reported 17 of the violations;
2. SERC reported that URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violation which SERC considered a mitigating factor, as discussed above;
4. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. SERC determined that the violations of CIP-007-1 R1 and R2 (SERC201000678 and SERC201000734) posed a serious or substantial risk to the reliability of the BPS, as discussed above;
6. URE implemented certain above and beyond compliance measures, as discussed above; and
7. 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 two hundred fifty thousand dollars ($250,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[25] *See* 18 C.F.R. § 39.7(d)(4).

[26] *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).

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.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Andrea B. Koch* Director of Compliance and Analytics SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org	Sonia C. Mendonça* Associate 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* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net 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 Maggie A. Sallah* Senior Counsel James M. McGrane* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 494-7778 (704) 494-7787 (704) 357-7914 – facsimile msifontes@serc1.org msallah@serc1.org 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
Associate 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
Senior Counsel and Associate Director, Enforcement Processing
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
edwin.kichline@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments