PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2013

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

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

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because 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-003, CIP-004, CIP-005, CIP-006, CIP-007, CIP-008, and CIP-009. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred ninety-eight thousand dollars ($198,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers SERC2011006592, SERC2011008277, SERC2011008278, SERC201000523, SERC2011006594, SERC2011007430,

[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.

SERC2012010943, SERC2011008279, SERC2011006597, SERC2012010945, SERC2012010946, SERC2011006595, SERC2011006596, SERC2011006598, SERC2011006599, SERC2011006600, SERC2011006601, SERC2011006602, SERC2011006603, SERC2012010949, and SERC2011008283 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 16, 2013, by and between SERC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2236	SERC2011006592	CIP-002-1	R3	High	$198,000
			SERC2011008277	CIP-003-1	R4	Medium	
			SERC2011008278	CIP-003-1	R5	Lower	
			SERC201000523	CIP-004-1	R4	Lower	
			SERC2011006594	CIP-005-1	R1	Medium	
			SERC2011007430	CIP-005-1	R2	Medium	
			SERC2012010943	CIP-005-3a	R3	Medium	
			SERC2011008279	CIP-005-1	R4	Medium	

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2236	SERC2011006597	CIP-006-1	R1	Medium	$198,000
			SERC2012010945	CIP-006-1	R2	Medium	
			SERC2012010946	CIP-006-1	R3	Medium	
			SERC2011006595	CIP-007-1	R1	Medium	
			SERC2011006596	CIP-007-1	R2	Medium	
			SERC2011006598	CIP-007-1	R3	Lower	
			SERC2011006599	CIP-007-1	R4	Medium	
			SERC2011006600	CIP-007-1	R5	Lower	
			SERC2011006601	CIP-007-1	R6	Lower	
			SERC2011006602	CIP-007-1	R7	Lower	
			SERC2011006603	CIP-007-1	R8	Lower	
			SERC2012010949	CIP-008-3	R1: R1.4	Lower	
			SERC2011008283	CIP-009-1	R1	Medium	

CIP-002

The purpose statement of Reliability Standard CIP-002 provides:

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities[4] should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.
>
> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

[Footnote added.]

SERC2011006592 CIP-002-1 R3

CIP-002-1 R3 provides:

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

[4] 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.

modeling, and real-time inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics;

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

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

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

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

URE submitted a Self-Report stating that it had a violation of CIP-002-1 R3. While URE was preparing for its annual Cyber Vulnerability Assessment (CVA), it discovered two switches in an Electronic Security Perimeter (ESP) that were essential to the operation of Critical Assets but were not included on the CCA list. These switches were added to the ESP and were not being afforded all of the protective measures of CCAs within an ESP. While URE did have a written process for identifying these CCAs, the lack of sufficient detail in the written process resulted in a greater opportunity for overlooking necessary actions.

SERC determined the duration of the violation to be from when the switches were added to the ESP, through when the switches were added to the CCA list.

SERC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the two switches were not being afforded all of the protective measures of CCAs within an ESP, which put them at a greater risk of being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS. URE did have a written process for identifying CCAs; however it contained insufficient detail which led to the exclusion of the two switches from the CCA list, despite their being located within an ESP.

CIP-003

The purpose statement of Reliability Standard CIP-003 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect

Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

SERC2011008277 CIP-003-1 R4

CIP-003-1 R4 provides:

> Information Protection — The Responsible Entity shall implement and document a program to identify, classify, and protect information associated with Critical Cyber Assets.
>
> > R4.1. The Critical Cyber Asset information to be protected shall include, at a minimum and regardless of media type, operational procedures, lists as required in Standard CIP-002, network topology or similar diagrams, floor plans of computing centers that contain Critical Cyber Assets, equipment layouts of Critical Cyber Assets, disaster recovery plans, incident response plans, and security configuration information.
> >
> > R4.2. The Responsible Entity shall classify information to be protected under this program based on the sensitivity of the Critical Cyber Asset information.
> >
> > R4.3. The Responsible Entity shall, at least annually, assess adherence to its Critical Cyber Asset information protection program, document the assessment results, and implement an action plan to remediate deficiencies identified during the assessment.

CIP-003-1 R4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it had a violation of CIP-003-1 R4. The Self-Report contained two instances. SERC determined that URE failed to document the results of the annual review for adherence to its CCA information protection program. SERC also determined that URE failed to protect the CCA information within URE's configuration management database (CMDB), which is used to document all critical and non-critical Cyber Assets and access points to the ESPs that have been identified. The CMDB tool was restricted to approximately 380 information technology (IT) personnel.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when the CCA information was afforded protection.

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 document the assessment results and action plan could have resulted in deficiencies not being remediated. Failing to protect CCA information properly could expose the CCAs to a cyber security attack, increasing the risk to CCAs being compromised and rendered inoperable. Access to the CMDB required authorization and user credentials such as a user identification (ID) and password. There were no identified deficiencies in the CCA information assessment.

SERC2011008278 CIP-003-1 R5

CIP-003-1 R5 provides in pertinent part:

> Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.
>
> R5.1.1. Personnel shall be identified by name, title, business phone and the information for which they are responsible for authorizing access.
>
> R5.1.2. The list of personnel responsible for authorizing access to protected information shall be verified at least annually.
>
> R5.2. The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.
>
> R5.3. The Responsible Entity shall assess and document at least annually the processes for controlling access privileges to protected information.

CIP-003-1 R5 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had a violation of CIP-003-1 R5. SERC determined that URE failed to include, as part of the annual review of access privileges to protected information, 60 individual personnel with access to CCA information. These individuals had not been included on the CCA information access list.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE added the personnel to the CCA information access control list.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. While personnel were missing from the CCA information access list, each had properly been granted access based upon their roles and responsibilities.

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.

SERC201000523 CIP-004-1 R4

CIP-004-1 R4 provides in pertinent part:

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

CIP-004-1 R4 and R4.1 have a “Lower” VRF and a “Moderate” VSL. CIP-004-1 R4.2 has a “Medium” VRF.

URE submitted a Self-Report stating that it had a violation of CIP-004-1 R4. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE failed to revoke access to CCAs within seven calendar days for a service vendor employee who no longer needed such access. The employee left the vendor company on good terms. However, URE was not notified of the employee's departure until a month later, at which time electronic access to the CCAs was revoked. URE had no record of this vender employee requesting a remote access code, which was required in order to gain electronic remote access, during the time of this violation.

URE self-reported that it failed to update the list of personnel with authorized cyber access to CCAs within seven calendar days for several individuals. Eighty-eight employees on an access list had electronic access to CCAs but were not on the access list.

URE self-reported that on two separate occasions it failed to ensure access lists were properly maintained and updated within seven calendar days of any change. Two employees had electronic access to CCAs but had not been placed on the access list. Additionally, two individuals were placed on the access list that did not require electronic access to the CCAs.

URE self-reported that a contractor erroneously received access to a PSP without receiving authorization. This individual worked on the custodial staff as a contractor and required access to two PSPs based on the roles and responsibilities associated with the job function. Although the employee had a completed personnel risk assessment (PRA) and cyber security training, access was granted to one of the PSPs without approved authorization. The contractor had unauthorized physical access for approximately 41 days. The contractor was approved for authorized access to the PSP on the same day the incident was discovered.

SERC determined the duration of the violation to be from the date the individuals were excluded from the authorized list, through when the CCA lists were corrected.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All of the individuals at issue had cyber security training, had a completed PRA, were in good standing, and had not been terminated for cause.

CIP-005

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."

SERC2011006594 CIP-005-1 R1

CIP-005-1 R1 provides in pertinent part:

> Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).
> >
> > R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
> >
> > R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.

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

CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4, and R1.5 have a "Medium" VRF and a "Severe" VSL. CIP-005-1 R1.6 has a "Lower" VRF.

URE submitted a Self-Report stating that it had a violation of CIP-005-1 R1. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

SERC determined that URE failed to afford five Cyber Assets used in the electronic access control and/or monitoring (EACM) of the ESP the protective measures of CIP-004 R3, CIP-007 R1, and CIP-007 R3 through R9, specified in CIP-005 R1.5.

URE self-reported that it failed to designate devices as access points within the ESP. Twenty-six access points were Cyber Assets that had network connections that crossed the ESP boundary. The Cyber Assets were used for monitoring and logging of security events or intrusion events.

URE self-reported multiple instances associated with CIP-005 R1. The first instance involved an employee who obtained electronic access to two EACM devices without proper approval. Access to these devices aligned with the employee's job function and was based on a need. The second incident involved two EACM devices that were not identified as access points to the ESP. The third instance involved 39 EACMs that were not afforded the protective measures as required by CIP-005 R1.5. The 39 EACMs consisted of 34 firewalls, 4 servers, and 1 logging device. SERC learned that 34 firewalls were not afforded any of the required protections. URE failed to review and update access to shared accounts in the event of personnel changes for four servers and a logging appliance as required by CIP-007 R5.2.3. SERC determined that URE failed to identify the access points due to insufficient processes and procedures.

During a Compliance Audit, SERC determined that URE failed to identify and document access points for the energy management system (EMS) that resided within the ESP. SERC learned that approximately 59 access points were involved. The access points were serially connected between the front-end processors and field remote terminal unit (RTU).

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when the devices were identified as access points in the ESP.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, a lack of processes, procedures, and proper tools to identify and document electronic access points greatly increased the risk of CCAs being compromised and rendered inoperable. Failing to identify and protect EACM devices could introduce vulnerabilities to the ESP and the CCAs located therein.

SERC2011007430 CIP-005-1 R2
CIP-005-1 R2 provides:

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

R2.5.2. The authentication methods.

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

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

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

URE submitted a Self-Report to SERC stating that it had a violation of CIP-005-1 R2. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE used a remote virtual private network (VPN) for vendors and contractors to connect to the corporate network, which provided access to one ESP. If an individual was not assigned to a group profile, the individual would be denied access to ESP control systems and the EMS. URE temporarily modified an ESP access point configuration during severe weather conditions. URE modified the access control list. Although explicit-deny access lists were created to block access to control systems, URE omitted the explicit-deny rule for the EMS ESP, which allowed unauthorized access to the EMS.

URE self-reported several incidents regarding the controls established for remote access to the ESPs. The first incident was related to the implementation of strong procedural and technical mechanisms to address the authenticity of personnel with electronic access to the ESPs. SERC reviewed the URE's cyber security procedure and determined that it did not specifically address how the authentication server would be used as an access control mechanism to access the ESPs remotely. However, the authentication server was validating credentials for remote users accessing the ESPs. The second incident involved URE failing to review the authorization rights of administrators for all electronic access points to the ESPs. While some quarterly reviews occurred, not all of the electronic access points were included. The third incident involved a VPN device that controls remote access to ESP that was not configured to deny access by default.

URE self-reported that controls established for access to certain ESPs were not sufficient to ensure the authenticity of the accessing party at the access point. SERC determined that URE utilized multi-factor authentication for remote external access and multiple levels of authentication at the operating system and application levels in order to restrict access to specific user accounts. However, the multi-

factor authentication was applied only to remote interactive access attempts to the corporate network and not to interactive access attempts into the ESP originating from within the corporate network. SERC determined that URE failed to ensure that controls existed to verify the authenticity of interactive access to the ESPs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when the firewall access control list (ACL) configurations were modified.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, omitting the explicit-deny rule for the EMS gave users, who did not have cyber security training or PRAs, unauthorized access to the EMS ESP. Improperly configuring a VPN allowed nine users, who had cyber security training and PRAs, to have unrestricted access into the ESP. This greatly increased the risk of CCAs being compromised and rendered inoperable at a time when the system was already stressed. Failing to implement and document organizational processes and strong technical and procedural mechanisms to ensure the authenticity of users accessing the ESPs could have resulted in unauthorized individuals gaining access to CCAs.

SERC2012010943 CIP-005-3a R3

CIP-005-3a R3 provides:

> Monitoring Electronic Access — The Responsible Entity shall implement and document an electronic or manual process(es) for monitoring and logging access at access points to the Electronic Security Perimeter(s) twenty-four hours a day, seven days a week.
>
> R3.1. For dial-up accessible Critical Cyber Assets that use non-routable protocols, the Responsible Entity shall implement and document monitoring process(es) at each access point to the dial-up device, where technically feasible.
>
> R3.2. Where technically feasible, the security monitoring process(es) shall detect and alert for attempts at or actual unauthorized accesses. These alerts shall provide for appropriate notification to designated response personnel. Where alerting is not technically feasible, the Responsible Entity shall review or otherwise assess access logs for attempts at or actual unauthorized accesses at least every ninety calendar days.

CIP-005-3a R3 has a “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Report stating it had a violation of CIP-005- R3. During a scheduled network outage, URE failed to conduct logging and monitoring for approximately 28 hours. Although some of URE's logging and monitoring devices were running during the timeframe of this incident, the devices at issue did not perform logging and monitoring.

SERC determined the duration of the violation to be from when the outage occurred, through when URE resumed monitoring and logging activity.

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 monitor access to the ESPs 24 hours a day, seven days a week could result in unauthorized access attempts going undetected by URE, which increases the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS. The period of the violation was 28 hours. URE had access control policies in place that required multiple layers of authentication to gain access to the ESP.

SERC2011008279 CIP-005-1 R4
CIP-005-1 R4 provides in pertinent part:

> Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings; and

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

CIP-005-1 R4, R4.2, R4.3, R4.4, and R4.5 have a "Medium" VRF and a "Severe" VSL. CIP-005-1 R4.1 has a "Lower" VRF.

URE submitted a Self-Report stating that it had a violation of CIP-005-1 R4. An annual CVA was not performed for two access points to an ESP, and the network management community strings were not reviewed for specific access points. After further review, SERC determined that the two access points were firewalls, and that they had not been included in three annual CVAs. URE also failed to assess the network management community strings for 12 Cyber Assets in two annual CVAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE completed the CVA for the two 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 perform a comprehensive CVA for all access points, as well as failing to assess network management community strings within the ESP, could allow unauthorized access to Cyber Assets, resulting in the Cyber Assets being compromised and/rendered inoperable. Network community strings were restricted to authorized personnel and were changed annually. There were no reportable Cyber Security Incidents during the period of this violation.

CIP-006

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

SERC2011006597 CIP-006-1 R1

CIP-006-1 R1 provides:

> 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).

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-006-2 R2 provides in pertinent part:

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

R2.1. Be protected from unauthorized physical access.

R2.2. Be afforded the protective measures specified in Standard CIP-003-2; Standard CIP-004-2 Requirement R3; Standard CIP-005-2 Requirements R2 and R3; Standard CIP-006-2 Requirements R4 and R5; Standard CIP-007-2; Standard CIP-008-2; and Standard CIP-009-2.

CIP-006-1 R1 and CIP-006-2 R2.2 each have a "Medium" VRF and a "High" VSL. CIP-006-1 R1.8 has a "Lower" VRF.

URE submitted a Self-Report stating that it had a violation of CIP-006-1 R1. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE did not afford the protective measures of CIP-004 R3, CIP-007 R5.1.3, CIP-007 R1-R3 and CIP-007 R5-7, and CIP-009 to 27 devices that made up the Physical Access Control Systems (PACS).

URE self-reported two incidents. The first incident involved walls that did not reach the ceiling which were utilized to create a six-wall boundary in a PSP. The second incident was failing to maintain continuous escorted access of visitors within a PSP. A contractor was performing an upgrade on PSP security hardware and became separated from the designated escort. The separation occurred several times for approximately 24 minutes. For 12 of the 24 minutes, the unescorted contractor was in view of a security camera. URE personnel reviewed camera footage and observed no questionable actions from the contractor.

URE self-reported that it failed to identify multiple devices utilized to provide access to a PSP. According to URE, it discovered components of the PACS that had not been afforded any of the protections of CIP-006-1 R1.8. SERC learned 61 devices were involved.

URE self-reported that 10 shared accounts were not appropriately managed and secured in accordance with CIP-007 R5.2.3. URE resolved the issue by updating the passwords for these accounts. In

addition, URE's documented recovery plan for PACS did not meet all of the requirements of CIP-009. The recovery plan did not include language specific to the device type and did not address events of varying durations and levels of severity.

URE self-reported that it failed to maintain continuous escorted access of visitors within a PSP. SERC learned that two contract employees without unescorted access in a PSP became separated from their designated escort. This incident occurred for approximately three minutes.

URE self-reported that it had two incidents of failure to follow documented visitor control program procedures and it failed to perform an annual review on the physical security plan. The first incident occurred when two visiting vendors entered a PSP through an open door and URE failed to escort continuously. A plant employee, who was authorized to have unescorted access to that PSP, spotted the vendors one minute after they entered the PSP, and immediately escorted the vendors out of the PSP. The plant employee then had the vendors complete the necessary visitor logging documentation for re-entry and provided the continuous escort function within the PSP. The second visitor program incident occurred when an authorized unescorted URE employee allowed a visitor to go unattended for approximately three minutes while within the PSP when the visitor left the escort to walk to the restroom. The visitor was a URE employee who was transferring to this location and was shadowing the escort until approval was granted for authorized unescorted physical access.

URE reported that it failed to perform an annual review and update on its physical security plan. SERC reviewed the revision history of the physical security plan and discovered that documentation was reviewed and approved in the year prior and the year after.

During a Compliance Audit, SERC determined that URE failed to deploy alternative measures to control physical access where a completely enclosed six-wall border could not be established at a PSP. SERC found two openings at a PSP that did not have the required enclosed six-wall border, or alternative measures where a complete enclosure was not physically possible. The two openings were located between the hard ceiling and the enclosed wall barriers and had the dimensions of 19.5 X 8.0 Inches and 8.5 X 27 inches, which were not large enough to gain entrance easily into the PSP. SERC determined that URE failed to maintain a physical security plan, as required.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when changes were made to the PSP.

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 protect PACS devices could result in unauthorized

individuals gaining access to CCAs, which could impact the BPS. Incomplete six-wall borders coupled with non-continuous escorted access increased the risk of CCAs being compromised and/or rendered inoperable. There were other mechanisms in place to monitor and limit access, such as physical security personnel, closed circuit television, and card readers, and there was no easy access to the gaps in the PSP perimeter.

SERC2012010945 CIP-006-1 R2

CIP-006-1 R2 provides:

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

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

URE submitted a Self-Report stating it had a violation of CIP-006-1 R2. The issuance of physical access cards to personnel was not being managed in accordance with URE's internal physical security policy. Physical access cards are assigned to personnel, including contractors, and contain the photo identification and the encode number, which is the primary identification string that provides credentials to the PACS card reader device and therefore, access to CCAs and Cyber Assets within the PSPs.

URE did not maintain an accurate inventory of the encode numbers that were previously assigned to personnel that no longer required physical access to secured areas. As a result, the reissuance of the encode number to cards other than the one that it was initially associated with provided individuals with access into the PSP without approved authorization.

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

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Failure to manage access to the PSP could result in unauthorized malicious personnel gaining physical access to CCAs and Cyber Assets. This greatly increased the risk of CCAs being compromised and rendered inoperable.

SERC2012010946 CIP-006-1 R3
CIP-006-1 R3 provides:

> Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:
>
> > R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
> >
> > R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

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

SERC sent URE an initial notice of a Compliance Audit. URE submitted a Self-Report stating that it had a violation of CIP-006-3c R5. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

The initial Self-Report referred to two instances of CIP-006-3c R5. According to URE, an employee discovered that one of the doors at a PSP was not sending a "door ajar" alarm to the PACS. URE notified the vendor of the alarm malfunction, which the vendor fixed two days after the malfunction. SERC learned that URE was not able to identify the exact time or cause of the alarm's malfunction. The second incident occurred during scheduled network maintenance. According to URE, the corporate security control center, which hosts the assets that monitor physical access, lost communications with the devices monitoring physical access at physical access points to two PSPs. During this outage, an alarm notification was displayed to the security officer on duty which displayed a set of instructions, requiring access points within the PSPs to be physically monitored by URE personnel. SERC learned that the security officer failed to execute instructions generated by the alarm to dispatch personnel to the physical access points impacted. As a result, two PSPs were not being monitored for approximately five hours.

During the Compliance Audit, SERC determined that URE failed to implement the technical and procedural controls for monitoring physical access at all access points to PSPs 24 hours a day, seven days a week. A PSP door failed to generate an alarm indicating that it had been forced opened. The alarm was repaired the same day.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE fixed the PSP alarm door.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PSPs were staffed by security officers 24 hours a day, seven days a week and were secured access card readers limiting physical access. The locks and badge readers for the PSP doors were fully functional, limiting access to personnel with an authorized access card. Access to the PSPs involved was controlled during the single instance. Despite the failing to alarm, the doors remained physically secure.

CIP-007

The purpose statement of Reliability Standard CIP-007 provides:

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

SERC2011006595 CIP-007-1 R1

CIP-007-1 R1 provides:

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

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

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R1. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE's cyber security test procedures included a process to perform functional testing of new Cyber Assets and significant changes to existing Cyber Assets. The test procedures also required the test results to be documented and reported to information technology (IT) operations personnel. However, the test procedures did not include steps to determine whether cyber security controls were impacted by new Cyber Assets or significant changes to existing Cyber Assets within the ESP, as required.

URE self-reported two instances where it failed to follow cyber security test procedures and failed to ensure that testing was done in a manner that reflects the production environment. Three servers were involved in the first instance. Security patches for the servers were issued, but instead of testing the patches in a version-specific test environment, URE tested them in an older version's test environment. With regard to the second incident, a technician used a retired test checklist as a guide

to install patches on the EMS workstations and servers. As a result, a generic account was installed within the EMS production environment.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when the procedures were updated to ensure security controls were tested for each category of assets.

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 establish and/or follow test procedures for Cyber Assets within the ESPs could have adversely affected existing cyber security controls. In addition, failing to test Cyber Assets in a manner that reflects the production environment could allow security vulnerabilities to go undetected. This could have resulted in CCAs being compromised and/or rendered inoperable. All of the Cyber Assets within the ESP resided within an established PSP. The PSP was monitored by security officers 24 hours a day, seven days a week, and secured access card readers limited physical access. URE had access control policies in place that required multiple layers of authentication to gain access to the ESP.

SERC2011006596 CIP-007-1 R2

CIP-007-1 R2 provides:

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

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

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R2. While performing an internal review of its CIP-007 controls, URE discovered that its process for determining hardening of baseline ports and services did not adequately identify the ports and services required for normal and emergency operations. As a result, URE failed to assess ports and services for 20 CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE updated procedures used to install assets on the ESP to include a review of ports/services against the existing baseline.

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, un-assessed ports and services left the 20 CCAs within the ESP susceptible to security vulnerabilities. This could have resulted in the CCAs being compromised and/or rendered inoperable. However, the affected CCAs resided behind secured firewalls, which restricted any outside remote electronic access, meaning any compromise would have to occur from within the secured ESP.

SERC2011006598 CIP-007-1 R3

CIP-007-1 R3 provides:

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

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

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R3. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE was unable to confirm that all security patches had been evaluated within the required 30 days after their release. Additionally, security patches associated with third-party applications had not been installed on 196 Cyber Assets. For those Cyber Assets missing those third-party security patches, URE had not implemented and documented compensating measures.

URE self-reported that it failed to evaluate a collection of patches within the required 30 days after their release. URE would receive an e-mail notification from this particular vendor regarding the issuance of new security patches. Due to a change in email addresses for the company, email notifications were not received for three months.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE documented, evaluated, tested, and implemented the patches.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Out-of-date security patches could have allowed unauthorized electronic access to CCAs. In addition, failing to assess the security patches could result in vulnerabilities remaining unaddressed for extended periods of time, which increased the risk of a successful cyber attack against CCAs essential to the operation of the BPS.

SERC2011006599 CIP-007-1 R4

CIP-007-1 R4 provides:

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

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

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

URE submitted a Self-Report to SERC stating that it had a violation of CIP-007-1 R4. While reviewing its compliance with the CIP-007 Standards, URE discovered that 81 Cyber Assets were technically infeasible of having antivirus software and malware prevention tools. SERC reviewed URE's anti-malware process that was active during the timeframe of the Self-Report, and determined that the process addressed the installation of antivirus software and malicious software prevention tools; testing and installation of signatures; and contained compensating measures to mitigate risks in cases where antivirus or malware prevention tools could not be installed.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE submitted the Technical Feasibility Exceptions (TFEs).

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The TFEs were filed 28 days late. The 81 Cyber Assets had compensating measures in place, such as intrusion detection systems and intrusion prevention systems (IDS/IPS). Additionally, the other devices in the ESP were capable of installing malware prevention tools and had antivirus software installed to detect and prevent the propagation of malware.

SERC2011006600 CIP-007-1 R5

CIP-007-1 R5 provides:

> Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.

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

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

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

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

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

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

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

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

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

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

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

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

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R5. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE did not have documented processes of technical and procedural controls for 85 shared accounts (R5), did not maintain a list of designated personnel for approving user accounts (R5.2), and failed to perform annual reviews to verify access privileges for two calendar years (R5.1.3). In addition, URE failed to enforce password controls for 16 CCAs (R5.3) and failed to ensure that user accounts are implemented by designated personnel (R5.1.1).

URE self-reported two instances where it failed to manage access to generic accounts associated with Cyber Assets and CCAs within an ESP. URE failed to add a vendor to the list of individuals with access to a shared account. URE also failed to maintain documentation of a shared generic user account, which was installed on two network switches that are CCAs.

URE self-reported two instances where it failed to change passwords for default accounts prior to the devices going into service and to change local account passwords on at least an annual basis. URE did not change three account passwords associated with 41 Cyber Assets at least annually and failed to retain documentation that default accounts were changed on 54 devices prior their deployment into production.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when the three account passwords associated with the 41 Cyber Assets were changed.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to implement technical and procedural controls for shared, administrator, and generic accounts could allow an attacker to access or compromise CCAs, resulting in URE's network becoming inoperable, which could significantly impact the BPS.

SERC2011006601 CIP-007-1 R6

CIP-007-1 R6 provides:

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

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

URE submitted a Self-Report stating it had a violation of CIP-007-1 R6. While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE discovered that 17 CCAs and seven Cyber Assets did not have the required agent installed to monitor system events. URE used a security information and event management device to monitor system events. As a result, the event logs were not sent to the security information and event management device but were being stored locally for approximately one day and then being over-written with new events.

URE self-reported that it discovered five CCAs that did not have automated tools or organizational process controls in place to monitor system events. The five devices, which were servers, did not have the required agent installed to monitor system events. As a result, the event logs were not sent to the security information and event management device but were being stored locally for approximately one day and then being over-written with new events.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor system events that are 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 compromised or rendered CCAs inoperable, which could significantly impact the BPS. All of the Cyber Assets within the ESP resided within an established PSP. The PSP was staffed by security officers 24 hours a day, seven days a week and were secured access card readers limiting physical access. URE had access control policies in place that required multiple layers of authentication to gain access to the ESP.

SERC2011006602 CIP-007-1 R7

CIP-007-1 R7 provides:

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

CIP-007-1 R7 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R7. While performing an internal review of its CIP-007 controls, URE discovered it had failed to implement formal methods, processes, and procedures for disposal and redeployment of two types of Cyber Assets — front end processors (FEPS) and the PACS assets. In addition, SERC learned that URE did not have records to confirm that data on the hard drive of an EMS workstation was destroyed or erased prior to its disposal.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when the procedures were created to address the Cyber Assets' disposal and redeployment.

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 follow the disposal procedure for a hard drive containing EMS data and failing to have disposal and redeployment procedures for two types of Cyber Assets within the ESP could have resulted in the unauthorized retrieval and the exposure of sensitive cyber security and/or reliability data used to support the EMS network, information logs, and historical events. This could introduce malicious activity causing significant impact to the BPS. However, none of the device types that lacked the disposal and redeployment procedures were disposed of or redeployed during the period of this violation—indicating that disposal or redeployment of such devices occurs infrequently. In addition, the hard drive had failed, making it more difficult for unauthorized recovery of data from the device.

SERC2011006603 CIP-007-1 R8

CIP-007-1 R8 provides:

> 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-007-1 R8 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it had a violation of CIP-007-1 R8. The required CVAs were not performed for three years on 35 CCAs. URE had established documents identifying the vulnerability assessment process; however, the process was not followed, and the 35 CCAs were missed.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE conducted a CVA that included the CCAs.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to perform complete CVAs may have led to a failure to identify systems or components at risk within the ESP. In addition, failing to mitigate known vulnerabilities placed the CCAs and the BPS at risk.

CIP-008

The purpose statement of Reliability Standard CIP-008-3 provides: "Standard CIP-008-3 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008-23 [sic] should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

SERC2012010949 CIP-008-3 R1: R1.4

CIP-008-1 provides in pertinent part:

> Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
>
> *****

> R1.4. Process for updating the Cyber Security Incident response plan within thirty calendar days of any changes.

CIP-008-3 R1 has a "Lower" VRF and a "High" VSL.

URE submitted a Self-Report stating that it had two instances of a violation of CIP-008-3 R1. URE failed to update its Cyber Security Incident response plan (CSIRP) with the correct contact information specific to the manager role. The manager transitioned to a new role. The manager's name was not removed from the CSIRP and replaced with the new contact information within 30 days.

Changes that had been made to the sabotage and cyber incident detection, analysis, and reporting process (Process), which is part of the CSIRP, was not updated within 30 calendar days. SERC learned that the changes to the document title and the website link were made, but the CSIRP was not updated until approximately four months later.

SERC determined the duration of the violation to be from when the CSIRP should have been updated, through when URE updated the CSIRP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. If the CSIRP needed to be executed, the phone number designated to reach the desk of the manager was correct. Personnel responsible for the execution of the Process document were aware of the name change and location of the updated document, and in the event of an emergency, they would have been involved in execution of the plan. No Cyber Security Incidents were reported during the timeframe of the incidents.

CIP-009

The purpose statement of Reliability Standard CIP-009-1 provides: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

SERC2011008283 CIP-009-1 R1

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:

R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).

R1.2. Define the roles and responsibilities of responders.

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

URE submitted a Self-Report stating that it had a violation of CIP-009-1 R4.[5] While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the self-reported violation.

URE self-reported that while performing the annual recovery plan exercise, it discovered that it did not have a recovery plan addressing four servers.

Domain controllers were listed as CCAs on URE's CCA list and were being afforded the protective measures of CCAs. However, these domain controllers were not included in URE's recovery plan. They were not included because URE considered domain controllers as non-essential for recovery of core systems.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE created the recovery plans for the servers.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although it may have taken more time, URE's core systems could have been restored without the domain controllers and the four servers.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred ninety-eight thousand dollars ($198,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC considered URE's compliance history as an aggravating factor in penalty determination;

[5] During SERC's assessment, it became apparent that the incident was a violation of CIP-009 R1 not CIP-009 R4.

2. URE self-reported the violations of CIP-002-1 R3, CIP-003-1 R4 and R5, CIP-004-1 R4, CIP-005-1 R2 and R4, CIP-005-3a R3, CIP-006-1 R2, CIP-007-1 R1 through R8, CIP-008-3 R1, and CIP-009-1 R1;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SERC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of CIP-003-1 R5, CIP-004-1 R4, CIP-006-1 R3, CIP-007-1 R4, CIP-008-3 R1, and CIP-009-1 R1 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. the violations of CIP-002-1 R3, CIP-003-1 R4, CIP-005-3a R3, CIP-005-1 R4, CIP-006-1 R1, and CIP-007-1 R1, R2, R6, and R7 posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
8. the violations of CIP-005-1 R1 and R2, CIP-006-1 R2, and CIP-007-1 R3, R5, and R8 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
9. URE took above-and-beyond actions, which SERC took into consideration when assessing the proposed penalty;[6] and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

[6] URE allocated 23 personnel dedicated to supporting compliance with NERC's CIP Standards. URE initiated a project regarding its internal system, which is used to manage both physical and electronic access to CIP assets. The system tracks requests for access, requests for removal of access, and the approvals required for such access. URE has begun a project to replace its current PACS. Once integrated into the present information technology environment, it will provide URE with enhanced reporting for CIP areas, greater flexibility managing access, reduced maintenance, enhanced security with the use of proximity smart badges, and increased visibility for the central security control center. URE's total cost for these improvements will be approximately $4.5 million dollars.
URE will also conduct a third-party assessment of its current processes and procedures to ensure compliance with CIP-005 R1, R2, and R3.2. The assessment will include the steps needed to achieve compliance with Version 5 of CIP-005 R.1 and R.2. URE shall implement those third-party suggestions that URE and SERC mutually agree are necessary, effective, and appropriate to improve the reliability of the BPS. URE will submit an action plan to SERC for each mutually agreed upon action arising from the third-party report. The timing of implementation of any recommendation shall be mutually agreed upon between URE and SERC. SERC will monitor URE's implementation of this commitment in accordance with the NERC Compliance Monitoring and Enforcement Program.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred ninety-eight thousand dollars ($198,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[7]

SERC2011006592 CIP-002-1 R3

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT006169-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions as detailed in its Mitigation Plan:

1. Updated the CCA list to include the two switches;
2. Performed physical inspections of all Critical Asset facilities and confirmed that all of the CCAs had been properly identified and documented;
3. Modified the CCA list to indicate the owner of each CCA;
4. Identified information and/or topics to be considered for inclusion in the annual cyber security training to provide greater awareness with respect to ESP and CCA requirements;
5. Updated the CIP-002 R3 processes to include written steps to ensure that all changes to the ESP are evaluated prior to reconfigurations to determine the potential impacts to an ESP and/or CCA list; and
6. Conducted training of applicable personnel on the updated CIP-002 R3 processes.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011008277 and SERC2011008278 CIP-003-1 R4 and R5

URE's Mitigation Plan to address its violations of CIP-003-1 R4 and R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008119-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions as detailed in its Mitigation Plan:

[7] *See* 18 C.F.R § 39.7(d)(7).

1. Expanded the annual review of adherence to the program under CIP-003 R4.3 to include a verification of access privileges to certain samples of the CCA information to confirm that privileges were appropriately applied to that sampled CCA information;
2. Documented an attestation following the annual CIP-003 R4.3 assessment noting that no deficiencies were identified in the assessment;
3. Included administrator and other support accounts, and the personnel with access to these accounts, in the annual review of access privileges to protected CCA information under CIP-003 R5.2;
4. Isolated and restricted access to information pertaining to network assets stored in the configuration management database, based on URE's needs and appropriate to personnel roles and responsibilities;
5. Updated the CIP-003 R4 process to a) include a clearer description of specific expectations for the assessment of adherence to URE's information protection program, and b) require documentation of the action plan to remediate deficiencies identified in the assessment;
6. Circulated the updated CIP-003 R4 process to appropriate personnel;
7. Updated CIP-003 R5 process with sufficiently detailed steps to ensure the inclusion of all administrative and support accounts in the CIP-003 R5.2 annual review;
8. Circulated the updated CIP-003 R5 process to appropriate personnel as needed; and
9. Conducted training of CCA information owners and IT administrators on the enhanced CIP-003 R4 and R5 processes, addressing the importance of conducting annual sampling and validation of access privileges and including all administrative and support accounts in the annual reviews.

URE certified that the above Mitigation Plan requirements were completed.

SERC201000523 CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT004035 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. On a monthly basis, verify that the CCA access list listing the vendor's employees is consistent with the access list maintained by the EMS vendor. These verifications shall be completed

within each month and continue for three months. Results of the verification process will be documented; and

2. Conduct training to ensure employees working with the EMS vendor employees understand their role in the process of granting and denying access to CCAs.

URE certified that the above Mitigation Plan requirements were completed.

In addition to the actions required by its Mitigation Plan, URE completed the following additional actions to mitigate the full scope of its violation of CIP-004-1 R4:

1. Remedied all identified discrepancies in existing CCA access lists;
2. Implemented a process requiring a quality assurance review for all unescorted physical access grants, and communicated this to affected employees;
3. Updated the process to grant and remove electronic access for the PACS, which assigns a single person the responsibility of granting access in the source system and completing the form which updates the necessary CCA access list; and
4. Circulated the updated process to affected personnel to ensure awareness.

URE attested the above mitigation activities were completed.

SERC2011006594, SERC2011007430, and SERC2011008279 CIP-005-1 R1, R2, and R4
URE's Mitigation Plan to address its violations of CIP-005-1 R1, R2, and 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 SERCMIT008245-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions as detailed in its Mitigation Plan:

1. Updated and circulated as training its CIP-004 R4, CIP-005 R1-R5, CIP-007 R1, CIP-007 R3, CIP-007 R4, CIP-007 R5, CIP-007 R6, CIP-007 R8, and CIP-007 R9 procedures;
2. Conducted PRAs as necessary;
3. Updated discrepant access lists, default "deny all" lists, and documentation;
4. The CIP common checklists were updated, the requirement to use was documented, and it was circulated;
5. Two EACM systems that were missed in the CVA were assessed;

6. Documentation reviews for the EACM systems were performed;
7. A default "deny all" filter was applied on select group policies on the VPN device that controls external interactive access to the ESP network segments;
8. A review was performed to identify any additional access points to the ESP;
9. One EACM system that was not afforded necessary protections as specified in CIP-005 R1.5 was shut down;
10. A mechanism for evidencing password changes for shared accounts was documented;
11. A list of all third-party applications running in the EACM environments was compiled;
12. Added a review of VPN filters to the quarterly review of firewall access control lists;
13. Assessed the two access points missed in the CVA;
14. Identified ports required for operations and monitoring of Cyber Assets through VPN devices, and updated ports/services documentation;
15. Implemented and tested appropriate access control list restrictions;
16. Completed implementation of protective measures identified under CIP-005 R1.5 for the IDS/IPS system;
17. Identified and documented the serial access points in the CMDB, and the annual CVA included a review of all serial access points to ensure all points were identified;
18. Updated the appropriate ESP drawings with the serial access points;
19. Removed the CIP filter;
20. Reviewed and modified the appropriate access point firewall ACL configurations to remove destination subnets used for rules that may include addresses where no hosts exist;
21. Modified the request for change template to specify only host-to-host communications allowed on CIP firewalls ACLs;
22. Performed training sessions on the audit finding. Specifically, causes and process changes implemented to avoid similar issues were discussed;
23. Modified the access point firewall VPN ACL configuration to remove the entry allowing non-CIP authorized access into the ESP;
24. Performed training sessions on the audit finding. Specifically, causes and process changes implemented to avoid similar issues were discussed; and

25. Conducted a review of people who could potentially access Cyber Assets through the non-CIP authorization server to ensure that those given access because of this issue should actually have access.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010943 CIP-005-3a R3

URE's Mitigation Plan to address its violation of CIP-005-3a 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 SERCMIT008675-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Required a board member to review future changes that could require additional post change testing related to logging and monitoring. This person has familiarity with the CIP requirements, the architecture of the EACM system(s), how changes in the network would impact those systems either directly or indirectly, and an understanding of the changes that are being submitted;
2. Enabled the silent log source detection feature of the logging and monitoring system for the purpose of aiding the identification of certain CIP assets that are not logging or monitoring;
3. Corrected the routing to include the missed network segments; and
4. Held a meeting to discuss the updated CIP-005 ESP procedure with network infrastructure personnel. That procedure was then circulated more broadly to ensure awareness, and this awareness was considered training.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011006597 and SERC2012010945 CIP-006-1 R1 and R2

URE's Mitigation Plan to address its violations of CIP-006-1 R1 and R2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008674-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Created a list of persons with electronic access to the PACS;

2. Documented the division of responsibilities regarding the PACS;
3. Performed a full review of the PACS to ensure all components that authorize or log access are included as in-scope;
4. Created a list of shared accounts with electronic access to the PACS;
5. Changed PACS shared account passwords;
6. Documented a mechanism for evidencing those shared password changes;
7. Created and circulated a detailed recovery plan for the PACS;
8. Finalized ports/services baseline;
9. Began assessing security patches internally;
10. Identified and documented all third-party applications;
11. Verified that PACS assets were reporting to the security information and event management device;
12. Stopped reissuing encode numbers;
13. Provided new access cards coded with a unique encode number to all persons with PSP access;
14. Ensured that all gaps in the PSP six-wall boundaries were remedied and the physical security plan was updated, and created a checklist to document the existence of the six-wall boundary for new or modified PSPs;
15. Completed the CIP-006 physical security plan annual review;
16. Established a program to prompt the initiation and completion of that annual review, and the visitor control program was updated;
17. Updated and circulated the CIP-004 R4, CIP-006 R1-R8, CIP-007 R1, CIP-007 R3, CIP-007 R5, CIP-007 R6, CIP-007 R7, and CIP-009 R1-R5 procedures;
18. Held a meeting with the PACS vendor to ensure all PACS components were included as in scope for the CIP-006 R2.2 requirements; and
19. Provided on-going awareness communications and training to key personnel regarding the importance of proper escorting of visitors (including employees) within PSPs.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010946 CIP-006-1 R3

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008199-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Sent an awareness communication regarding escorting visitors;
2. Updated and circulated the visitor control program;
3. Completed the annual review of the physical security program;
4. Established a process to prompt the initiation and completion of the physical security plan annual review;
5. Disciplined the security officer who failed to initiate the action plan;
6. Gave an emphasis reminder regarding procedures to all security guards at the control center;
7. Gave an emphasis reminder regarding the manually monitoring of PSPs in the event of an alarm malfunction to all personnel in the corporate security department;
8. Sent an awareness communication to all personnel with physical and cyber access to CIP assets regarding their responsibility to not prop open PSP doors, among other things;
9. Sent an awareness email sent to all physical area owners regarding a series of security-related posters;
10. Trained all physical area owners on their responsibility regarding visitor control and continuous escorting;
11. Presented to officers, senior managers, and managers regarding the importance of the CIP escorting requirements and the expectations of management leadership on the topic; and
12. Provided additional guidance to each person with access to CCAs on the importance of appropriate visitor escorting, specifically focusing on the escorting of URE employees.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011006595, SERC2011006596, SERC2011006598, SERC2011006599, SERC2011006600, SERC2011006601, SERC2011006602, and SERC2011006603 CIP-007-1 R1 through R8

URE's Mitigation Plan to address its violation of CIP-007 R1 through 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 SERCMIT005572 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Revised the CIP-007 R1 through R9 procedures to improve processes and promote consistency, and circulated those updated procedures to ensure awareness;
2. Documented the division of responsibility for FEPs;
3. Created and implemented checklists to ensure new assets, or existing assets undergoing changes, were compliant with the CIP-007 Requirements;
4. Created a list of third-party applications running in the transmission and generation environments;
5. Installed a "like" device of the AV/patching and event logging servers with operating systems in the test environment;
6. Removed the disabled id from the impacted EMS workstations and servers;
7. Revoked the technician's physical and electronic access to CIP Assets;
8. Implemented all of the event logging server agents on the ICCP and micro-servers;
9. Assessed the security patches in question;
10. Generated patch assessment reports;
11. Removed the application with the associated account;
12. Deleted the generic account;
13. Changed the passwords on all switches and routers;
14. Began using configuration management to document password changes on switches, routers, and firewalls; and
15. Formally documented the requirement to use the CIP common checklist and provided appropriate communication to network administrators on its importance.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010949 CIP-008-3 R1: R1.4

URE's Mitigation Plan to address its violation of CIP-008-3 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008488 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Updated the CSIRP to reflect:
    a. The new manager; and
    b. The document that replaced the process document; and
2. Communicated to the incident response team that all changes to personnel and documentation that may affect the CSIRP should be communicated to IT security.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011008283 CIP-009-1 R1

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008201-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Created a recovery plan for transmission domain controllers;
2. Created a recovery plan for four servers;
3. Circulated updated recovery plans to affected personnel to ensure awareness;
4. Updated the CIP-009 R1 through R5 recovery plan for CCAs procedure, which provides direction those creating or maintaining recovery plans, to provide:
    a. Examples of scenarios of varying duration and severity; and
    b. Examples of media that should be tested, including spare electronic components or equipment, written documentation of configuration settings, tape backups, etc.;

5. Circulated the updated CIP-009 R1 through R5 recovery plan for CCAs procedure to affected personnel to ensure awareness;
6. Verified that all CCAs have a recovery plan, including those CCAs not needed for system restoration;
7. Provided training on the new asset checklists which reference the CIP-009 activities to be performed for all newly installed CIP Assets;
8. Circulated an awareness communication to affected personnel requiring the use of the CIP-common checklist for adding or replacing Cyber Assets and the CIP common checklist for adding or replacing Cyber Assets networks, when installing or replacing a Cyber Asset; and
9. Provided additional training to those involved in the installation steps and requisite compliance tasks with regard to new CIP Assets, focusing on CIP-009 requirements.

URE certified that the above Mitigation Plan requirements were completed.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a one hundred ninety-eight thousand dollar ($198,000) 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.

[8] *See* 18 C.F.R. § 39.7(d)(4).
[9] *North American Electric Reliability Corporation*, "Guidance Order on Reliability Notices of Penalty," 124 FERC ¶ 61,015 (2008); *North American Electric Reliability Corporation*, "Further Guidance Order on Reliability Notices of Penalty," 129 FERC ¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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

1. SERC considered URE's compliance history as an aggravating factor in penalty determination, as discussed above;
2. URE self-reported the violations of CIP-002-1 R3, CIP-003-1 R4 and R5, CIP-004-1 R4, CIP-005-1 R2 and R4, CIP-005-3a R3, CIP-006-1 R2, CIP-007-1 R1 through R8, CIP-008-3 R1, and CIP-009-1 R1;
3. URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SERC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of CIP-003-1 R5, CIP-004-1 R4, CIP-006-1 R3, CIP-007-1 R4, CIP-008-3 R1, and CIP-009-1 R1 posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. the violations of CIP-002-1 R3, CIP-003-1 R4, CIP-005-3a R3, CIP-005-1 R4, CIP-006-1 R1, and CIP-007-1 R1, R2, R6, and R7 posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
8. the violations of CIP-005-1 R1 and R2, CIP-006-1 R2, and CIP-007-1 R3, R5, and R8 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
9. URE took above-and-beyond actions, which SERC took into consideration when assessing the proposed penalty, as discussed above; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred ninety-eight thousand dollars ($198,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between SERC and URE executed December 16, 2013, included as Attachment a;

1. Disposition Document for Common Information to Instant Violations, included as Attachment a-1;[10]
2. Disposition Document for CIP-002-1 R3 (SERC2011006592), included as Attachment a-2;
3. Disposition Document for CIP-003-1 R4 (SERC2011008277), included as Attachment a-3;
4. Disposition Document for CIP-003-1 R5 (SERC2011008278), included as Attachment a-4;
5. Disposition Document for CIP-004-1 R4 (SERC201000523), included as Attachment a-5;
6. Disposition Document for CIP-005-1 R1 (SERC2011006594), included as Attachment a-6;
7. Disposition Document for CIP-005-1 R2 (SERC2011007430), included as Attachment a-7;
8. Disposition Document for CIP-005-3a R3 (SERC2012010943), included as Attachment a-8;
9. Disposition Document for CIP-005-1 R4 (SERC2011008279), included as Attachment a-9;
10. Disposition Document for CIP-006-1 R1 (SERC2011006597), included as Attachment a-10;
11. Disposition Document for CIP-006-1 R2 (SERC2012010945), included as Attachment a-11;
12. Disposition Document for CIP-006-1 R3 (SERC2012010946), included as Attachment a-12;
13. Disposition Document for CIP-007-1 R1 (SERC2011006595), included as Attachment a-13;
14. Disposition Document for CIP-007-1 R2 (SERC2011006596), included as Attachment a-14;
15. Disposition Document for CIP-007-1 R3 (SERC2011006598), included as Attachment a-15;
16. Disposition Document for CIP-007-1 R4 (SERC2011006599), included as Attachment a-16;
17. Disposition Document for CIP-007-1 R5 (SERC2011006600), included as Attachment a-17;
18. Disposition Document for CIP-007-1 R6 (SERC2011006601), included as Attachment a-18;
19. Disposition Document for CIP-007-1 R7 (SERC2011006602), included as Attachment a-19;
20. Disposition Document for CIP-007-1 R8 (SERC2011006603), included as Attachment a-20;

[10] The disposition documents order follows the order discussed in the filing and not the numbering on the disposition documents.

21. Disposition Document for CIP-008-3 R1; R1.4 (SERC2012010949), included as Attachment a-21;
22. Disposition Document for CIP-009-1 R1 (SERC20110082830), included as Attachment a-22;

b) Record documents for the violation of CIP-002-1 R3, included as Attachment b:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT006169-1;
   3. URE's Certification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-003-1 R4, included as Attachment c:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT008119-1;
   3. URE's Certification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-003-1 R5, included as Attachment d:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT008119-1;
   3. URE's Certification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-004-1 R4, included as Attachment e:
   1. URE's Self-Reports;
   2. URE's Mitigation Plan designated as SERCMIT004035;
   3. URE's Certification of Mitigation Plan Completion attestation;

f) Record documents for the violation of CIP-005-1 R1, included as Attachment f:
   1. URE's Self-Reports;
   4. SERC's Source document;
   5. URE's Mitigation Plan designated as SERCMIT008245-1;
   2. URE's Certification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-005-1 R2, included as Attachment g:
   1. URE's Self-Reports;
   2. SERC's Source document;

3. URE's Mitigation Plan designated as SERCMIT008245-1;
4. URE's Certification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-005-3a R3, included as Attachment h:
1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008675-1;
3. URE's Certification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-005-1 R4, included as Attachment i:
1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008245-1;
3. URE's Certification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-006-1 R1, included as Attachment j:
1. URE's Self-Reports;
2. SERC's Source document;
3. URE's Mitigation Plan designated as SERCMIT008674-1;
4. URE's Certification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-006-1 R2, included as Attachment k:
1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008674-1;
3. URE's Certification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-006-1 R3, included as Attachment l:
1. URE's Self-Report;
2. SERC's Source document;
3. URE's Mitigation Plan designated as SERCMIT008199-1;
4. URE's Certification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-007-1 R1, included as Attachment m:
1. URE's Self-Reports;

2. URE's Mitigation Plan designated as SERCMIT005572;
3. URE's Certification of Mitigation Plan Completion;

n) Record documents for the violation of CIP-007-1 R2, included as Attachment n:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-007-1 R3, included as Attachment o:
   1. URE's Self-Reports;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

p) Record documents for the violation of CIP-007-1 R4, included as Attachment p:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-007-1 R5, included as Attachment q:
   1. URE's Self-Reports;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

r) Record documents for the violation of CIP-007-1 R6, included as Attachment r:
   1. URE's Self-Reports;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

s) Record documents for the violation of CIP-007-1 R7, included as Attachment s:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT005572;
   3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005572;
3. URE's Certification of Mitigation Plan Completion;

u) Record documents for the violation of CIP-008-3 R1; R1.4, included as Attachment u:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008488;
3. URE's Certification of Mitigation Plan Completion;

v) Record documents for the violation of CIP-009-1 R1, included as Attachment v:

1. URE's Self-Reports;
2. URE's Mitigation Plan designated as SERCMIT008201-1; and
3. URE's Certification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Marisa A. Sifontes* General Counsel Maggie A. Sallah* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org msallah@serc1.org	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net John R. Twitchell* VP and Chief Program Officer SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8205 (704) 357-7914 – facsimile jtwitchell@serc1.org

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

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments