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-006-3 R1, CIP-005-2 R3, CIP-004-3 R2, CIP-007-1 R5, CIP-006-3a R6, CIP-005-3 R1, CIP-006-1 R1, CIP-007-3 R3, CIP-006-1 R3, CIP-007-1 R2, CIP-009-1 R5, CIP-005-3a R2, CIP-005-3a R5, CIP-004-3 R4 and CIP-007-3 R6 . According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred and ten thousand dollars ($110,000), 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

[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 (2011). *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.

Numbers SERC2011007156, SERC2011007385, SERC2011007531, SERC2011007532, SERC2011008616, SERC2011008775, SERC2012010143, SERC2012010793, SERC2012010343, SERC2012010344, SERC2012010346, SERC2012010549, SERC2012011380, SERC2012011584, and SERC2013011678 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 20, 2013, by and between SERC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	URE	NOC-2234	SERC2011007531	CIP-004-3	R2	Lower	$110,000
			SERC2012011584	CIP-004-3	R4	Lower	
			SERC2011008775	CIP-005-1	R1	Medium	
			SERC2012010549	CIP-005-3a	R2	Medium	
			SERC2011007385	CIP-005-2	R3	Medium	
			SERC2012011380	CIP-005-3a	R5	Lower	
			SERC2012010143	CIP-006-1	R1	Lower	
			SERC2011007156	CIP-006-3a	R1	Medium	
			SERC2012010343	CIP-006-1	R3	Medium	
			SERC2011008616	CIP-006-3a	R6	Lower	

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	URE	NOC-2234	SERC2012010344	CIP-007-1	R2	Medium	$110,000
			SERC2012010793	CIP-007-3	R3	Lower	
			SERC2011007532	CIP-007-1	R5	Lower	
			SERC2013011678	CIP-007-3	R6	Medium	
			SERC2012010346	CIP-009-1	R5	Lower	

CIP-004

The purpose statement of Reliability Standard CIP-004 provides in pertinent part:

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

SERC2011007531 CIP-004-3 R2

CIP-004-3 R2 provides:

> R2. Training — The Responsible Entity[4] shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.
>
> > R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their

[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.

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

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

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

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

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

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

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

[Footnote added.]

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

URE submitted a Self-Report to SERC stating that it had a violation of CIP-004-3. Personnel were given access to a Critical Cyber Asset (CCA) prior to receiving the required cyber security training.

Two contractors were given remote electronic access to a shared account. The shared account accessed an application that resided on four CCAs. URE discovered the two contractors had not completed URE's cyber security training prior to accessing the shared account.

SERC determined the duration of the violation to be from when the users were given access to the CCA without cyber security training, through when the users completed cyber security training.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). The users' access to the CCAs was limited to "read-only," and each had completed a personnel risk assessment (PRA).

SERC2012011584 CIP-004-3 R4

CIP-004-3 R4 provides:

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

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

URE submitted a Self-Report stating that it had a violation of CIP-004-3 R4. Physical access to CCAs at one Physical Security Perimeter (PSP) for three contractors was not revoked within seven calendar days.

URE requested removal of physical access to CCAs for three contractors because they no longer had a business need for access. The contractors did not have electronic access to CCAs. URE revoked the physical access rights for one contractor six days late and for the other two contractors 19 days late.

Prior to the actual removal from the access list, URE had one of the contractors resolve an issue that required the contractor physically access CCAs. The other two individuals did not attempt to access the CCAs.

SERC determined the duration of the violation to be from seven days after personnel no longer required access to the CCAs, through when access for all three contractors was revoked.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The three contractors had completed PRAs and cyber security training. The revocation was

not due to termination for cause but requested because the contractors were no longer working on a project at the PSP.

CIP-005

The purpose statement of CIP-005 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

SERC2011008775 CIP-005-1 R1

CIP-005-1 R1 provides:

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

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

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

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

SERC sent URE an initial notice of a Compliance Audit. URE submitted a Self-Report that it was in violation of CIP-005-3 R1 because it unintentionally created an unauthorized access point to an Electronic Security Perimeter (ESP).

URE declassified an ESP subnet containing CCAs as a non-ESP. This required two CCAs, switches, to be moved to a new ESP subnet prior to the other subnet being declassified. URE changed the internet protocol (IP) addresses of the switches; however, URE mistakenly created an access point that did not require access via its secure remote access application.

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 it unintentionally created three unauthorized access points. Three servers inside an ESP were accessible from a separate private network. This configuration resulted in the unintentional creation of three ESP access points. After this discovery, URE closed the access points.

URE self-reported that it had identified four undocumented access points. The undocumented ESP access points were switches. URE was performing work on the ESP that involved removing non-ESP IP addresses from the switches and configuring new ESP IP addresses on the switches. Instead of removing the non-ESP access points, they became ESP IP addresses, which resulted in the creation of access points.

URE self-reported that it failed to afford one or more of the protective measures of CIP-005 R1.5 to four electronic access control and/or monitoring systems (EACMs). Four EACMs, two firewall management servers, and two servers that were used to configure secure ports on switches, were involved. URE failed to afford these devices the protections of CIP-007 R1, R3, R4, and R5.3.

During the Compliance Audit SERC determined that URE failed to identify the access points associated with all devices terminating within the ESP. URE had serial point-to-point devices from the energy management system (EMS) control center to remote field locations. Because these devices communicate across an ESP, they are required to be identified and documented as access points. URE also utilized mixed trust network switches with ESP and non-ESP virtual local area networks. These switches had externally connected communications and terminated within the ESP. Therefore, they should have been identified as access points. There were a total of 149 devices involved

During the Compliance Audit SERC determined that URE did not afford the protective measures as specified in CIP-005 R2 and CIP-007 R5 to EACMs, as required. URE failed to implement access rules at its electronic access points that restricted traffic to only the ports and services that were required for operations and for monitoring Cyber Assets within the ESP. Additionally, the devices were not capable of enforcing the password requirements required by CIP-007-1 R5.3 and URE had not filed a Technical Feasibility Exception (TFE).

SERC determined that URE had a violation of CIP-005-1 R1 because it failed to identify all access points to the ESPs.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to identify and protect access points could allow unauthorized access to CCAs, which greatly increased the risk of CCAs being compromised and rendered inoperable.

For the first instance, the affected device was not directly exposed to connectivity outside URE's control systems network. For the second instance, access to the devices was controlled by the firewall access control lists. The four individuals with access had completed PRAs and cyber security training. For the third instance, the Cyber Assets were not directly exposed to connectivity outside URE's control systems network. Anyone trying to access the switches had to present credentials and be granted authorization to that device. There were no other Cyber Assets connected to these switches. Additionally, logging was enabled on the switches; therefore, anyone denied access to the ESP device would have been logged. For the fourth and fifth instances, the ESPs where the devices resided utilized real-time monitoring, including an intrusion detection system (IDS). Additionally, serial device communication is asynchronous and non-routable in nature, which significantly reduces cyber vulnerabilities and the chance of exploitation. With regard to the sixth incident, while URE failed to file a TFE, it had procedural controls in place.

SERC2012010549 CIP-005-3a R2

CIP-005-3a R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> R2.3. The Responsible Entity shall implement and maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).
>
> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.
>
> R2.5. The required documentation shall, at least, identify and describe:
>
> R2.5.1. The processes for access request and authorization.
>
> R2.5.2. The authentication methods.
>
> R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004-3 Requirement R4.
>
> R2.5.4. The controls used to secure dial-up accessible connections.

CIP-005-3a R2 has a “Medium” VRF and a “Severe” VSL.

URE submitted a Self-Report to SERC stating that it had a violation of CIP-005-3a R2. A user was able to gain external interactive access through an ESP access point without using URE's remote access system to authenticate the accessing party.

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.

A firewall rule was modified to support a project for the deployment of new servers. The servers were non-critical Cyber Assets within an ESP. This rule change allowed a web browser from a corporate workstation to access a non-critical Cyber Asset inside an ESP. Access was granted via a port without authenticating through URE's primary remote access solution. URE updated the firewall's access control list to ensure the external interactive access used its primary remote access solution. SERC determined that URE failed to implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

URE self-reported that it failed to ensure authenticity of the accessing party through an electronic access point. URE enabled external interactive access for the purpose of testing a secondary authentication method. This allowed six virtual workstations located on a subnet outside an ESP access to Cyber Assets inside an ESP without authenticating through its primary remote access solution. URE failed to recognize that the configuration would allow staff to bypass the controls established by the production instance of its primary remote access solution. The six virtual workstations were shut down the day after the issue was identified, and the firewall rules were modified to prevent the information technology (IT) employee from accessing the ESP. SERC determined that URE failed to implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

SERC determined the duration of the violation to be from when the external interactive access was enabled without the implementation of strong procedural or technical controls at the access points, through when the external interactive access was disabled.

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 implement strong procedural or technical controls at the access points to authenticate the accessing party could result in unauthorized access to the ESP. Unauthorized access increased the risk to CCAs being compromised and rendered inoperable, which could impact BPS reliability. The interactive access was limited to a subset of IT support administrators with current PRAs and access to CCAs based on "need to know." The access was for non-critical Cyber Assets and did not allow a user to access CCAs.

SERC2011007385 CIP-005-2 R3

CIP-005-2 R3 provides:

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

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

URE submitted a Self-Report stating that it had a violation of CIP-005-2 R3. Access points (firewall) at an ESP were not transferring access logs to detect and alert for attempts at or actual unauthorized accesses to the ESP. 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 performs access point monitoring and alerting by configuring devices to send logs to a centralized monitoring, logging, and alerting system. URE changed the configuration of two firewalls, which resulted in logs not being sent to the centralized monitoring, logging, and alerting system. These firewalls protected three CCAs. Nine months after the configuration was changed, these firewalls were configured correctly and began to transfer logs to the centralized monitoring, logging, and alerting system.

URE self-reported that an access point was not transferring access logs to detect and alert for attempts at or actual unauthorized accesses to the ESP. URE performed a security-related operating system upgrade to an access point switch. During an update to its centralized monitoring, logging, and alerting system, URE discovered that the switch had not been sending security logs since the date of the security upgrade.

URE self-reported that it failed to perform monitoring and alerting on ESP access point logs. A firewall management server stopped transferring logs to the centralized monitoring, logging, and alerting system. Due to the loss of access point logs, the centralized monitoring, logging, and alerting system was unable to monitor or alert for 11 access points. URE restarted the server the same day, and the centralized monitoring, logging, and alerting system began receiving logs. SERC determined that URE failed to implement electronic or manual processes for monitoring and logging access at access points to the ESP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from when URE changed the firewall configuration, through when URE began to transfer logs to the monitoring, logging, and alerting system.

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 monitoring and alerting on access points could allow a Cyber Security Incident to go undetected. However, only three access points protecting four CCAs were affected by the first two incidents. The third incident occurred for less than an hour. No Cyber Security Incidents were known to have occurred during the violation period.

SERC2012011380 CIP-005-3a R5

CIP-005-3a R5 provides:

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

CIP-005-3a R5 has a “Lower” VRF and a “Lower” VSL.

URE submitted a Self-Report to SERC stating that it had a violation of CIP-005-3a R5. URE failed to retain all electronic access logs for at least 90 calendar days. 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 performed manual log reviews for a dial-up ESP access point because the switch was not capable of transferring logs automatically. URE performed a manual review of the logs for the switch. URE decommissioned this switch and erased the data storage media. URE attempted to retrieve the logs for the switch and discovered that the logs for five days had been deleted. These logs had not been retained for 90 days and had not been manually reviewed before being deleted.

URE self-reported that it failed to update an ESP diagram within 90 days of a change. URE identified the violation while it was planning the decommissioning of a group of network printers and discovered that one of the printers had already been removed. According to URE, a change request ticket was created for the printer's removal, but the change request was put on hold. The individual responsible for removing the printer was not aware of the hold and removed the printer. Because of the change request hold, the ESP diagram was not updated.

SERC determined the duration of the violation to be from when the logs were deleted without being retained for at least 90 calendar days, through when the diagram was updated.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Five days of logs were at issue for the switch before it was removed from the ESP. The switch had additional security measures that required a user to respond with a 40-digit encrypted passkey before granting access. The printer was a non-Critical Cyber Asset within an ESP and was removed from the ESP.

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."

SERC2012010143 CIP-006-1 R1

CIP-006-1 R1 provides:

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

R1.1. Processes to ensure and document that all Cyber Assets within an Electronic Security Perimeter also reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to the Critical Cyber Assets.

R1.2. Processes to identify all access points through each Physical Security Perimeter and measures to control entry at those access points.

R1.3. Processes, tools, and procedures to monitor physical access to the perimeter(s).

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

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

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

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

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005

Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

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

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

SERC sent URE an initial notice of a Compliance Audit.

URE submitted a Self-Report stating it was in violation of CIP-006-1 R1.8 because it failed to afford seven physical access control systems (PACS) the protective measures of CIP-006-1 R1.8. 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 identify seven card access controllers as PACS. Because of this, the devices were not afforded the protections of CIP-005 R2, CIP-005 R3, and CIP-007 R1, R2, R5.3, and R6. The devices were inside a PSP but were not protected by an ESP. SERC determined that URE failed to ensure that Cyber Assets used in the access control and monitoring of the PSPs were afforded the protective measures specified in CIP-003 through CIP-009, as required.

During the Compliance Audit, SERC determined that URE did not afford the protective measures as specified in CIP-005 R2 and CIP-007 R5 to PACS, as required. URE failed to implement access rules at the electronic access points that restricted traffic to only those ports and services required for operations and monitoring of the PACS. URE also failed to require enhanced passwords pursuant to CIP-007 R5. The passwords that did not meet the requirements were for all of URE's local accounts and the shared accounts for one business unit.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to protect PACS could allow an attacker to gain unauthorized physical access to degrade, disable, or misuse CCAs, which could impact BPS reliability. URE utilized intrusion detection and prevention systems to monitor for malicious activity. URE had procedural controls in place pursuant to CIP-007 R5.3 for all passwords in this business unit.

SERC2011007156 CIP-006-3a R1

CIP-006-3a R1 provides:

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

R1.1. All Cyber Assets within an Electronic Security Perimeter shall 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 such Cyber Assets.

R1.2. Identification of all physical 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. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

R1.5. Review of access authorization requests and revocation of access authorization, in accordance with CIP-004-3 Requirement R4.

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

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

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

R1.7. Update of the physical security plan within thirty calendar days of the completion 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. Annual review of the physical security plan.

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-3a R1.6. URE failed to log the entry time and exit time of a visitor to a PSP. URE utilized a manual visitor log sheet to document the exit and entry of visitors to the PSP in question. SERC reviewed the log entry, which contained the visitor's visit date, full name, company, and escort name. However, the entry was missing the time-in and the time-out information.

SERC determined the duration of the violation to be from when URE failed to document the entry time and the exit time of the visitor, through when the visitor left the PSP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The log entry documented the visitor's full name, escort, and date of entry and exit to and from the PSP. The visitor was continuously escorted by an authorized URE employee, and the visitor did not have access to CCAs.

SERC2012010343 CIP-006-1 R3

CIP-006-1 R3 provides:

R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:

R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.

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

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

During a Compliance Audit, SERC determined that URE had a violation of CIP-006-1 R3. URE failed to document and implement the technical and procedural controls for monitoring physical access to a PSP 24 hours a day, seven days a week. There were two incidents involved in the finding.

URE removed the reviewing and responding to alarms requirement from its procedure for monitoring physical access to all access points to the PSPs. Unauthorized access attempts for unauthorized or invalid badge swipes were logged in the PACS, but the PACS did not send email alerts to personnel on the distribution list, who are responsible for immediately reviewing and responding to the alarms. A PSP door to one operations center failed to produce an alarm and provide immediate notification to responsible personnel when forced open. SERC determined that URE failed to document and implement the technical and procedural controls for monitoring physical access at all access points to PSPs 24 hours a day, seven days a week.

While SERC was performing its assessment and determining the scope of the violation, it identified additional instances which expanded the scope of the violation.

URE self-reported that it did not immediately respond to a PSP held-door alarm. An employee exited a PSP access point door. The door did not close completely, resulting in a held-door alarm. An alarm email was generated and sent to a distribution list of alarm monitors. The personnel responsible for responding to the alarm failed to notice the held-door alarm email alert. The employee who exited the PSP returned through the same door and closed the door completely. About an hour later, personnel from the incoming shift noticed the alarm email and investigated the held-door alarm to find that the door was properly shut.

URE self-reported that it failed to immediately review unauthorized physical access alerts. According to URE, for eight days, URE performed maintenance on a door to a PSP. During this time period, URE deactivated the automated alarm email notifications and assigned a security guard to monitor the access point and manually log physical access. When the maintenance was completed on, URE ceased to have a security guard monitor the access point, but failed to reactivate the alarm email notifications. URE discovered the issue four days later, and re-activated the alarm email notifications. Eighty-six held-door alarms and five forced-door alarms were not responded to immediately during that four day period.

URE submitted an addendum explaining that, it had deactivated the automated alarm email notifications at another PSP. URE failed to respond to two force- door alarms during this time period. The instances occurred at three separate physical access points.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failing to respond immediately to forced open alarms or unauthorized access attempts combined with the removal of the reviewing and responding to alarms requirement from its procedure could have allowed unauthorized physical access to CCAs without triggering an alarm or logging the entry into the PSP. However, there was an established PSP for all of URE's sites with Critical Assets, and all of the physical access points were secured with either mechanical locks and/or electric locks to provide access control.

SERC2011008616 CIP-006-3a R6

CIP-006-3a R6 provides:

> R6. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
>
> - Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
> - Video Recording: Electronic capture of video images of sufficient quality to determine identity.
> - Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R4.

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

SERC sent URE an initial notice of a Compliance Audit. URE submitted a Self-Report stating that it was in violation of CIP-006-3a R6 because a log was generated that did not uniquely identify an individual who entered a PSP.

A security contractor allowed a custodian contractor to use another individual's badge to gain access to a PSP, which meant that the recorded log did not identify the correct individual. URE obtained an attestation from the security contractor that identified the individual who entered the PSP.

SERC determined the duration of the violation to be from when the log occurred that did not uniquely identify the individual, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The individual had authorized unescorted physical access, a current PRA, and cyber security training. Video camera recording was employed at the PSP access doors, which could be used to identify individuals uniquely.

CIP-007

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

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

SERC2012010344 CIP-007-1 R2

CIP-007-1 R2 provides:

> R2. Ports and Services — The Responsible Entity shall establish and document a process to ensure that only those ports and services required for normal and emergency operations are enabled.
>
> > R2.1. The Responsible Entity shall enable only those ports and services required for normal and emergency operations.
> >
> > R2.2. The Responsible Entity shall disable other ports and services, including those used for testing purposes, prior to production use of all Cyber Assets inside the Electronic Security Perimeter(s).

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

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

During a Compliance Audit, SERC determined that URE had a violation of CIP-007-1 R2. URE did not ensure that only those ports and services required for normal and emergency operations were enabled. URE could not disable unused ports on three clocks due to technical limitations. Because of this, URE should have filed a TFE documenting compensating measures.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The Cyber Assets involved only provide time synchronization for other devices in the ESP. Even though disabling of unused ports is not possible, the Cyber Assets cannot be used to communicate with devices in any other way or compromise the network. In addition, the ESP where the Cyber Asset resided utilized real-time monitoring, including an IDS.

SERC2012010793 CIP-007-3 R3

CIP-007-3 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003-3 Requirement R6, shall establish, document and implement a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).
>
> R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.
>
> R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure.

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

During a Compliance Audit, SERC determined that URE had a violation of CIP-007-3 R3. URE failed to assess all security patches for applicability within 30 calendar days of availability of such patches.

URE did not evaluate 19 security patches within the required 30 days after their release. Eighteen of these patches were applicable to server software that was introduced to URE's network. While URE had a patch management program in place, it failed to follow the program. With regard to the remaining security patch, SERC learned that URE relied on a third-party vendor for patch availability notifications. Because the third-party vendor issued a late notification of patch availability, URE failed to evaluate the security patch within 30 calendar days after its release, as required.

SERC determined the duration of the violation to be from when the software was introduced to URE's network without the patches having been evaluated, through when the missed patches were evaluated.

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 assess security patches within 30 days left the Cyber Assets susceptible to security vulnerabilities, which puts Cyber Assets used to operate the BPS at risk. However, as mitigating measures, URE used a combination of multiple levels of firewalls, network address translation, and filtering.

SERC2011007532 CIP-007-1 R5

CIP-007-1 R5 provides:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> > R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
> >
> > > R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

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

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

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

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

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

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

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

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

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

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

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

URE submitted a Self-Report that it had a violation of CIP-007-1 R5. URE failed to identify two individuals with access to a shared account. 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.

Two contractors were given remote electronic access to a shared account. URE failed to identify and document that these contractors had access to the shared account. The shared account accessed an application that resided on four CCAs. These contractors were given read-only access.

URE self-reported that it failed to change passwords at least annually, as required. Seventeen shared accounts were involved. URE failed to identify all the shared accounts, and personnel did not perform password changes in accordance with its established procedures.

URE self-reported that it failed to identify all individuals with access to shared accounts. URE failed to identify 14 EMS network support personnel with access to a shared account. The shared account provided administrative access to two ESP access points.

URE self-reported that it failed to change a password at least annually. According to URE, a local administrator password to a door card access controller had not been changed annually. The personnel responsible for keeping the login credentials updated were no longer employed by URE and had not updated the login credentials or provided the login credentials to the successive support personnel during the turnover. After discovering the issue, URE contacted the vendor, who was unable to reset the password because the controller was outdated.

SERC sent URE an initial notice of a Compliance Audit. URE self-reported that a password did not employ the use of special characters, as required. SERC learned that the shared account had access to 52 network device CCAs.

During the Compliance Audit, SERC determined that URE failed to implement enhanced password on local accounts. URE utilized a password management solution, which operates on workstations, servers, and network devices but not local accounts. SERC learned that the local accounts were not capable of enforcing the password requirements of CIP-007-1 R5.3 and URE had not filed a TFE. SERC determined that URE failed to implement enhanced passwords, as required.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement: 1) procedures to minimize and to manage the scope and use of shared accounts; and 2) enhanced passwords on all Cyber Assets within ESPs, greatly increased the risk to CCAs being compromised and rendered inoperable, which could have caused the loss of monitoring and control of the BPS. These devices were protected by an established PSP. No Cyber Security Incidents were known to have occurred for the period of the violation.

SERC2013011678 CIP-007-3 R6

CIP-007-3 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
>
> R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.
>
> 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-007-3 R6 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report that it had a violation of CIP-007-3 R6. Security status monitoring was not being performed for three devices. Three servers were involved, two of which were CCAs. URE performs security status monitoring by configuring devices to send logs to the centralized monitoring,

logging, and alerting system. URE moved two servers, both CCAs containing an intelligent remote management processor device, to production. The intelligent remote management processors were not configured to send logs to the centralized monitoring, logging, and alerting system. URE reset a non-critical serial console server and restored the factory default settings without reconfiguring the device to send logs to the centralized monitoring, logging, and alerting system. URE performed a scan on the ESP subnets and discovered that the three devices were not logging to the centralized monitoring, logging, and alerting system. URE configured the three devices to send logs to the centralized monitoring, logging, and alerting system.

SERC determined the duration of the violation to be when the devices were added that were not configured for security status monitoring, through when the devices were configured for security status monitoring.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to monitor system events that 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 rendered CCAs inoperable, resulting in the loss of monitoring and control of the BPS. In addition, URE's failure to log system events related to security events could have impaired its ability to conduct an incident response. The devices were located within a PSP and an ESP, and access was limited to personnel with authorized cyber access to these devices.

CIP-009

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

SERC2012010346 CIP-009-1 R5

CIP-009-1 R5 provides: "Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

CIP-009-1 R5 has a "Lower" VRF and a "Severe" VSL.

SERC sent URE an initial notice of a Compliance Audit. The SERC audit team reported that URE had a violation of CIP-009-1 R5. URE failed to show evidence that information essential to recovery that is stored on backup media had been tested at least annually to ensure that the information was available.

SERC learned that URE performed verification of the health and hardware status of the backup devices and hardware, but it did not perform testing of the information on backup media that is essential for the recovery of CCAs to validate the availability of the information. The violation affected 64 CCAs that were backed up to hard drives.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed daily backups of the devices. URE also performed monitoring of the backup system to test the readability of the backup media.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred ten thousand dollars ($110,000) 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 the penalty determination;
2. URE self-reported the violations of CIP-004-3 R2 and R4, CIP-005-3a R2, CIP-005-2 R3, CIP-005-3a R5, CIP-006-3a R1, and CIP-007-3 R6;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SERC considered to be a partially mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SERC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE took above-and-beyond actions concerning physical security, which SERC took into consideration when assessing the proposed penalty;[5] and

[5] URE is centralizing its physical monitoring activities into a single location. URE is standardizing its physical monitoring and access control systems via implementation of a new access control and video monitoring system. URE is working with a vendor to customize the new system so that it alarms based on a threshold for invalid card swipes and invalid personal identification number attempts. URE is also implementing a central security monitoring station for trained security guards who respond to access control system alarms.

8. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred ten thousand dollars ($110,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

SERC2011007531 CIP-004-3 R2
URE's Mitigation Plan to address its violation of CIP-004-3 R2 was submitted to. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005739-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Modify the applicable procedure; and
2. Issue communication stating requirements comply with CIP-004 R2 and R3.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012011584 CIP-004-3 R4
URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008770 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revoke the contractors' physical access;
2. Discipline the employee that did not process the revocation requests within the required timeframe; and

URE is also migrating to a single security badge system and upgrading all physical CIP access point doors with two-factor authentication card readers. In addition, URE performed an analysis of its substations that have the highest likelihood of malicious activity, and would also have the greatest impact on BPS reliability. As a result of the analysis, URE undertook a physical hardening project. URE has also replaced PSP doors at several locations, which will reduce the number of false door alarms as well as harden the physical access points to the secure areas.

[6] *See* 18 C.F.R § 39.7(d)(7).

3. Include an article in an internal newsletter reinforcing procedure usage for infrequently performed tasks.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011008775 CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 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 SERCMIT006729-3 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. Completed remaining network configuration changes which placed the CCAs on a secured ESP subnet.
2. Disable protocol;
3. Perform an extent of condition to ensure there were no other legacy protocols in use within URE's ESPs;
4. Disabled the ESP interface on the network switches;
5. Discipline the involved employees;
6. Coach the applicable employees on the importance of performing change plan steps in sequence;
7. Revise the departmental change management procedure with additional requirements to implementation plans to make sure that compliance steps are apparent and followed in the necessary sequence;
8. Provide an email communication addressing the new implementation plan requirements;
9. Revise procedure to include an additional barrier to help prevent potential unauthorized access points;
10. Provide interim guidance to operations information technology (OIT) personnel and contractors, who support changes involving EACMs;
11. Ensure the protections prescribed in CIP-005 R1.5 are applied to the identified EACM devices;
12. Perform an extent of condition to assess devices that perform access control/authentication and/or monitoring of electronic access points in order to validate their designation as EACM devices and correct any issues resulting from the extent of condition assessment;

13. Performed awareness training regarding EACM devices;
14. Revised the change management procedure;
15. Moved identified EACM devices into an ESP;
16. Performed an extent of condition review in the new environments to ensure that all externally connected serial communication end points terminating at any device with the ESP have been identified;
17. Performed any corrective actions, as needed; and
18. Revised applicable procedure to include additional guidance on classification of ESP access points.

URE will complete the following actions detailed in its Mitigation Plan:

1. Issue interim guidance instructing firewall policy administrators that while ports and services must be validated against the list of approved ports and services for the related destination devices in an ESP, the rules must not be combined into a single rule;
2. Revise the firewall policy management procedure;
3. Perform an extent of condition review in the new environments to ensure that all externally connected serial communication end points terminating at any device with the ESP have been identified;
4. Perform any corrective actions, as needed;
5. Revise applicable procedures to include additional guidance on the classification of ESP access points;
6. Perform an extent of condition review in the new environments to ensure that (non-legacy) firewall policies conform to the revised procedure;
7. Perform any corrective actions, as needed
8. Decommission devices within the legacy environments. Complete remaining network configuration changes, which placed the CCAs on a secured ESP subnet;
9. Disable protocol;
10. Perform an extent of condition review to ensure there were no other legacy protocols in use within URE's ESPs;
11. Disable the ESP interface on the datacenter network switches;
12. Discipline the involved employees;

13. Perform human performance error reviews with the involved employees;
14. Evaluate process and performance and coach personnel on the importance of performing change plan steps in sequence;
15. Provide interim guidance in the form of email communication. The communication covered the new implementation plan requirements;
16. Implement a revision to the departmental change management procedure to include further requirements to implementation plans to ensure compliance steps are apparent and followed in the necessary sequence; and
17. Implement the preceding through procedure revision, an additional barrier to help prevent potential unauthorized access points.

SERC2012010549 CIP-005-3a R2

URE's Mitigation Plan to address its violation of CIP-005-3a 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 SERCMIT007871 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Adjust the firewall rules;
2. Perform an assessment to determine which human performance tools were ineffective and which should have been used under the circumstance; and
3. Review URE's internal stop, think, act, and review process with applicable personnel.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011007385 CIP-005-2 R3

URE's Mitigation Plan to address its violation of CIP-005-2 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005575-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in the Mitigation Plan:

1. Corrected the configuration of the firewalls and network switches;
2. Performed refresher training for applicable personnel;

3. Added requirement to the departmental change management procedure;
4. Added checklist to RSA administration procedure;
5. Provided guidance communicating management expectation regarding end-point functional verification for significant changes and for the addition of new Cyber Assets;
6. Re-started the server; and
7. Implemented a new process for the periodic rebooting of the applicable server type.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012011380 CIP-005-3a R5

URE's Mitigation Plan to address its violation of CIP-005-3a 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 SERCMIT008636-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in Mitigation Plan:

1. Decommissioned all devices requiring manual log reviews at Critical Asset substations;
2. Provided lessons learned training to applicable personnel;
3. Modified the annual cyber security training to include more guidance regarding Critical Asset sites;
4. Updated the ESP drawing and the configuration management database to reflect the removal of the printer from the ESP;
5. Disciplined involved personnel; and
6. Implemented revisions to the change management process.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010143 CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007651-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in the Mitigation Plan:

1. Provide interim guidance to applicable and personnel and contractors who support changes involving PACs;
2. Applied protections prescribed in CIP-006 R1.8 to the identified PAC devices;
3. Performed an extent of condition to assess devices that perform access control/authentication and/or monitoring of physical access points in order to validate their designation as PACs devices and correct any issues resulting from the extent of condition assessment;
4. Provided an awareness training for PACs devices to applicable personnel;
5. Revised the change management procedure; and
6. Moved the identified PACs devices into an ESP.

URE will complete the following actions detailed in the Mitigation Plan:

1. Issue interim guidance instructing firewall policy administrators that while ports and services must be validated against the list of approved ports and services for the related destination devices in an ESP, the rules must not be combined into a single rule;
2. Revise the firewall policy management procedure;
3. Perform an extent of condition review in the new environments to ensure that all externally connected serial communication end points terminating at any device with the ESP have been identified;
4. Perform any corrective actions, as needed;
5. Revise applicable procedures to include additional guidance on the classification of ESP access points;
6. Perform an extent of condition review in the new environments to ensure that (non-legacy) firewall policies conform to the revised procedure;
7. Perform any corrective actions, as needed; and
8. Decommission devices within the legacy environments.

SERC2011007156 CIP-006-3a R1

URE's Mitigation Plan to address its violation of CIP-006-3a 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 SERCMIT007580 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Discipline the applicable personnel;
2. Send email to all personnel at the effected PSP restating the required visitor control steps; and
3. Perform refresher training on its visitor control program.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010343 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 SERCMIT010199 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in the Mitigation Plan:

1. Realigned the motion sensor;
2. Installed a working label near the sensor to notify personnel to not move or adjust the motion sensor;
3. Replaced the door with a standard design door, which does not allow the manual manipulation of the motion sensor;
4. Responded to the door alarm, which confirmed the event to be a false alarm and that no unauthorized personnel accessed the PSP;
5. Performed a human error performance review;
6. Reactivated the door alarm email notifications at the applicable sites; and
7. Revised the applicable procedures to include guidelines for suppressing/reactivating alarms or alarm email notifications and for ensuring zero-day testing is performed after door maintenance and prior to the removal of the alternative measures.

URE will complete the following actions detailed in the Mitigation Plan:

1. Perform an analysis to classify alarm events and define actions for response using a risk based approach. Revised applicable procedures to incorporate results of the analysis and a response to a set threshold of invalid personal identification number entries.

SERC2011008616 CIP-006-3a R6

URE's Mitigation Plan to address its violation of CIP-006-3a R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT006591-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revoke the physical access;
2. Conduct a meeting between URE and management at the security contractor to reinforce policy regarding badges and the need to notify URE regarding staff changes;
3. Obtain attestation from the security guard identifying the custodian contractor;
4. Follow up between URE management and management at the security contractor regarding the process for managing human error;
5. Train applicable personnel; and
6. Reinforce physical access rules with the custodian contract crew at the site where the violation occurred.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010344 CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010197-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. File a TFE with SERC documenting compensation measures;
2. Perform an extent of condition review to determine if issues exist at other URE sites; and
3. Correct any issues found.

SERC2012010793 CIP-007-3 R3

URE's Mitigation Plan to address its violation of CIP-007-3 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 SERCMIT010162 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Assess the missed patches;
2. Conduct a human performance review to evaluate the effective use of human performance tools;
3. Consolidate the security patch management processes into one process that does not rely on a third party for notification regarding patch releases; and
4. Train applicable personnel on the new process.

URE certified that the above Mitigation Plan requirements were completed.

SERC2011007532 CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005740-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE has completed the following actions detailed in the Mitigation Plan:

1. Ensured the user in question completes required cyber security training;
2. Implemented remote access authentication system;
3. Provided steps required prior to allowing read-only access;
4. Modified shared account management procedure to address process omission specific to shared account usage due to off-normal condition. Ensure that associated processes and procedures tie in to these modified processes;
5. Modified procedure to address process omission specific to shared account usage due to off-normal condition;
6. Issued communication stating URE requirements to comply with CIP-004 R2 and R3;
7. Reset out-of-date passwords;
8. Documented users of the identified shared account;
9. Reconciled accounts and passwords to a single controlled location (spreadsheet);

10. Established a named owner of the single account/password source;
11. Piloted an automated shared account password management tool;
12. Conducted an independent audit to determine accuracy (extent of condition) of the shared account spreadsheet and process;
13. Created a departmental procedure to define the process for identifying and recording shared accounts;
14. Conducted training on shared account management;
15. Implemented management of shared accounts using the automated tool, where possible;
16. Replaced door card access controller device;
17. Conducted a tabletop forum in which this occurrence and identified causes/missed opportunities are discussed and provide lessons learned to applicable employees;
18. Performed the corrective change to update the password on shared administrative accounts to a CIP complaint password;
19. Completed a human performance error review with the necessary personnel; and

Provided counseling to individuals and team members;

URE will take the following action detailed in its Mitigation Plan:

1. File TFEs for all devices which cannot technically enforce the requirements of CIP-007-3 R5.3.

SERC2013011678 CIP-007-3 R6

URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008769-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Configure the servers send logs to the centralized monitoring, logging, and alerting system;
2. Modify the change evaluation checklist to require the user to provide information; and
3. Discipline the employee, who submitted the change ticket request.

URE certified that the above Mitigation Plan requirements were completed.

SERC2012010346 CIP-009-1 R5

URE's Mitigation Plan to address its violation of CIP-009-1 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010167 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to revise the testing back-up media procedure to require restoration tests and the documentation of such tests.

URE certified that the above Mitigation Plan requirements were completed.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[8] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 23, 2013. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a one hundred ten thousand dollar ($110,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. SERC considered URE's compliance history as an aggravating factor in penalty determination, as discussed above;
2. URE self-reported the violations of CIP-004-3 R2 and R4, CIP-005-3a R2, CIP-005-2 R3, CIP-005-3a R5, CIP-006-3a R1, and CIP-007-3 R6;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;

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

4. URE had a compliance program at the time of the violations which SERC considered a partially mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SERC determined that the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE took above-and-beyond actions concerning physical security, which SERC took into consideration when assessing the proposed penalty, as discussed above; and
8. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred ten thousand dollars ($110,000) 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 20, 2013, included as Attachment a;
   1. Disposition Document for CIP-006-3a R1 (SERC2011007156), included as Attachment a-1;
   2. Disposition Document for CIP-005-2 R3 (SERC2011007385), included as Attachment a-2;
   3. Disposition Document for CIP-004-3 R2 (SERC2011007531), included as Attachment a-3;
   4. Disposition Document for CIP-007-1 R5 (SERC2011007532), included as Attachment a-4;
   5. Disposition Document for CIP-006-3a R6 (SERC2011008616), included as Attachment a-5;
   6. Disposition Document CIP-005-3 R1 (SERC2011008775), included as Attachment a-6;
   7. Disposition Document for CIP-006-1 R1 (SERC2012010143), included as Attachment a-7;
   8. Disposition Document for CIP-007-3a R3 (SERC2012010793), included as Attachment a-8;
   9. Disposition Document for CIP-006-1 R3 (SERC2012010343), included as Attachment a-9;

10. Disposition Document for CIP-007-1 R2 (SERC2012010344), included as Attachment a-11;
11. Disposition Document for CIP-009-1 R5 (SERC2012010346), included as Attachment a-12;
12. Disposition Document for CIP-005-3a R2 (SERC2012010549), included as Attachment a-13;
13. Disposition Document for CIP-005-3a R5 (SERC2012011380), included as Attachment a-14;
14. Disposition Document for CIP-004-3 R4 (SERC2012011584), included as Attachment a-15;
15. Disposition Document for CIP-007-3a R6 (SERC2013011678), included as Attachment a-16;

b) Record documents for the violation of CIP-006-3a R1, included as Attachment b:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT007580;
   3. URE's Certification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-005-2 R3, included as Attachment c:
   1. URE's Self-Reports;
   2. URE's Mitigation Plan designated as SERCMIT005575-1;
   3. URE's Certification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-004-3 R2, included as Attachment d:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT005739-1;
   3. URE's Certification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-007-1 R5, included as Attachment e:
   1. URE's Self-Reports;
   2. SERC's Source document;
   3. URE's Mitigation Plan designated as SERCMIT005740-2;

f) Record documents for the violation of CIP-006-3a R6, included as Attachment f:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT006591-2;
   3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Self-Reports;
2. SERC's Source document;
3. URE's Mitigation Plan designated as SERCMIT006729-3;

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

1. URE's Self-Report;
2. SERC's Source document;
3. URE's Mitigation Plan designated as SERCMIT007651-1;

i) Record documents for the violation of CIP-007-3a R3, included as Attachment i:

1. SERC's Source document;
2. URE's Mitigation Plan designated as SERCMIT010162;
3. URE's Certification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-006-1 R3, included as Attachment j:

1. URE's Self-Reports;
2. SERC's Source document;
3. URE's Mitigation Plan designated as SERCMIT010199;

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

1. SERC's Source document;
2. URE's Mitigation Plan designated as SERCMIT010197-1;

l) Record documents for the violation of CIP-009-1 R5, included as Attachment l:

1. SERC's Source document;
2. URE's Mitigation Plan designated as SERCMIT010167;
3. URE's Certification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-005-3a R2, included as Attachment m:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT007871;
3. URE's Certification of Mitigation Plan Completion;

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

1. URE's Self-Reports;
2. URE's Mitigation Plan designated as SERCMIT008636-2;
3. URE's Certification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-004-3 R4, included as Attachment o:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008770;
3. URE's Certification of Mitigation Plan Completion;

p) Record documents for the violation of CIP-007-3a R6, included as Attachment p:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT008769-1; and
3. URE's Certification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[9]

A copy of a notice suitable for publication is included in Attachment q.

[9] *See* 18 C.F.R § 39.7(d)(6).

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