December 30, 2014

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity 1 and Unidentified Registered Entity 2
FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity 1 (URE1), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 2 (URE2), 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 URE1 and URE2 (collectively, UREs) have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, the UREs neither admit nor deny the

[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 (2014). *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) and 18 C.F.R § 39.7(d).

[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.

violations, but have agreed to the assessed penalty of one hundred twenty thousand dollars ($120,000), 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 in this Full Notice of Penalty 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, which is included as Attachment A. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
SERC2013012483	CIP-002-1	R3	High/ Severe	URE1	$120,000
SERC2014013371	CIP-003-3	R6	Lower/ Severe		
SERC2013012237	CIP-004-3	R4	Lower/ High		
SERC2013011770	CIP-005-1	R1.1	Medium/ Severe		
SERC2013012498	CIP-005-1	R1.1	Medium/ Severe	URE2	
SERC2013012488	CIP-005-1	R1.5	Medium/ Severe	URE1	
SERC2013012496	CIP-005-1	R1.5	Medium/ Severe	URE2	
SERC2013011754	CIP-005-2	R1.5	Medium/ Severe	URE1	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Applicable Function(s)	Total Penalty
SERC2013012240	CIP-005-3a	R3	Medium/ Severe	URE1	$120,000
SERC2013011761	CIP-006-1	R1.1	Medium/ Severe		
SERC2013012242	CIP-006-1	R1.8	Medium/ Severe		
SERC2013012244	CIP-006-1	R1.8	Medium/ Severe	URE2	
SERC2013012490	CIP-006-1	R3	Medium/ Severe	URE1	
SERC2013012495	CIP-006-1	R3	Medium/ Severe	URE2	
SERC2013011763	CIP-006-3c	R5	Medium/ Severe	URE1	
SERC2013012486	CIP-007-1	R1	Medium/ Severe		
SERC2013012487	CIP-007-1	R2.2	Medium/ Severe		
SERC2013012532	CIP-007-1	R3	Lower/ Severe		
SERC2013012243	CIP-007-1	R6	Medium/ Severe		
SERC2013012489	CIP-007-1	R8.3	Medium/ Severe		
SERC2013012491	CIP-009-1	R1	Medium/ Severe		

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-002-1 R3 (SERC2013012483)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-002-1 R3. URE1 failed to identify all Critical Cyber Assets (CCAs) essential to the operation of its Critical Assets.

After an internal review, URE1 found workstations in separate Electronic Security Perimeters (ESPs) that it had originally classified as Cyber Assets within the ESP under CIP-005-1 R1.4 that it should have considered as CCAs under CIP-002-1 R3. Although not considered essential to the operation of the Critical Asset under its original assessment, these workstations did provide control capabilities and, if misused, could affect the operation of URE1's energy management system (EMS) and the bulk power system (BPS). SERC determined that URE1 was in violation of CIP-002-1 R3 because it failed to identify all CCAs that were essential to the operation of the Critical Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 added the misidentified Cyber Assets to the CCA list.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify Cyber Assets as CCAs could have left those devices without the required CIP protections, increasing the risk that the devices could be compromised and misused for malicious purposes. URE1 identified the workstations at issue as non-critical Cyber Assets within the ESP and protected them in the same manner it protected the identified CCAs. Use of the workstations required a user to be physically present at the workstations, and remote access was disabled. The first set of facilities, where approximately 90% of the workstations were deployed, were staffed 24 hours per day, seven days per week with operators and support staff as well as on-site security personnel. Moreover, a second set of facilities, containing approximately 10% of the workstations, had real-time security monitoring that included physical and logical access alarms and security cameras. URE1 had an intrusion detection system within the ESP monitoring for any port scans or pings against the EMS network. URE1 utilized a separate intrusion detection and prevention system on its ESP access point firewalls, behind which the workstations at issue resided. The workstations were within established ESPs and Physical Security Perimeters (PSP).

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. update its CIP-002 R3 procedure to include the concept of "compromise" in the CCA identification methodology because it was an identified root cause;
2. provide training to individuals affected by the update to the CIP-002 R3 procedure;
3. review and update the Cyber Asset/CCA list based on the updated CIP-002 R3 procedure;
4. update CIP-003 R6 procedures to address asset classification prior to the asset being implemented into production; and
5. provide training to individuals affected by the update to the CIP-003 R6 procedure.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-003-3 R6 (SERC2014013371)

URE1 submitted a Self-Report stating that it was in violation of CIP-003-3 R6. URE1 failed to follow its documented change control and configuration management process when updating malware prevention software on CCAs.

In URE1's change control and configuration management program, URE1 specified that any proposed changes hardware and software on Cyber Assets within the ESP should be documented through an internal change control management ticket which includes testing, approvals, and documentation. SERC determined that URE1 was in violation of CIP-003-3 R6 because it failed to follow its internal change control management process and updated malware prevention software on CCA workstations without following its documented change control and configuration management program.

SERC determined the duration of the violation to be from the date when URE1 mistakenly upgraded the malware prevention software without following its documented change control and configuration management process, until URE1 completed its testing of the cybersecurity controls.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 failed to follow its change control and configuration management program that allowed the implementation of untested changes to malware prevention software on CCAs. URE1 could have degraded existing cybersecurity controls or rendered the CCAs inoperable, reducing or eliminating URE1's ability to be aware of local system conditions or control its portion of the BPS. However, URE1 detected the update to the malware prevention software the following day and began investigating the scope of the issue. In addition, the change that URE1 implemented went through cybersecurity and functionality testing prior to deployment on corporate systems with no negative or adverse impacts to functionality or operations. URE1 also conducted after-the-fact testing and found no problems. System operators monitored the EMS 24 hours a day, seven days a week, and would have immediately noticed and reported to support personnel any system degradation. The EMS had security status monitoring in place to alert system administrators in the event the any malicious software was detected. The workstations were also within ESPs and PSPs, and physical and electronic access was limited to individuals who had completed personnel risk assessments and cybersecurity training.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. execute after-the-fact change control process;
2. analyze potential change control and configuration management sources of failure within groups that provide delegated operational support; and
3. develop and implement an action plan based on the results from the potential change control and configuration management sources.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-004-3 R4 (SERC2013012237)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-004-3 R4.1.

URE1 failed to update the list of personnel with access to CCAs within seven calendar days of any change of personnel with such access to CCAs, or any change in the access rights of such personnel. The violation involved two instances of failure. In both instances, the individuals had physical access only, and the revocation failures resulted from the failure of staff to follow the URE1 access revocation procedures after the individuals' retirement or resignation. SERC determined that URE1 was in violation of CIP-004-3 R4 (4.1 and 4.2) because it failed to update its list of personnel with access to CCAs within seven calendar days of any change of personnel with such access to CCAs, and it failed to revoke access to CCAs within seven calendar days for individuals who no longer required such access.

SERC determined the duration of the violation to be eight days after the first individual retired until URE1 updated the access list and revoked the first individual's access rights, and eight days after the second individual resigned until URE1 updated the access list and revoked the second individual's access rights.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to revoke access to CCAs could have allowed former employees to use their credentials to gain access to and sabotage CCAs. However, both employees would have to obtain a key through their former supervisors to gain entry through a perimeter barrier before they would have been able to use their physical access badge to access the PSP. Both employees were in good standing with URE1 prior to and after their departure. Neither employee used their cards to access any PSP or site after the date of their respective retirement and resignation. The revocation of access occurred six days and eleven days late, respectively.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. develop reinforcement training for individuals who have the ability to initiate off-boarding processes in the human resources system. The training would concentrate on the importance of timely data entry and possible compliance implications of late data entry;
2. develop training for managers who have direct reports with NERC CIP access. The training would concentrate on the importance and expectations of the manager's role in the off-boarding process;
3. implement reinforcement training in the learning management system; and
4. assign and schedule respective reinforcement training to be completed by any individuals identified.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-005-1 R1.1 (SERC2013011770)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-3a R1.1. URE1 failed to identify externally connected dial-up modems, terminating at devices within ESPs, as ESP access points.

URE1 had mistakenly identified the wrong devices as access points for some facilities' ESPs. Dial-up gateways secured, authorized, and managed remote access to the facilities, and once the security packets for the individuals accessing were authenticated at the gateways, modems permitted access to the CCA. Originally, URE1 had identified the gateways as access points. Instead, it should have identified the interior modems as the access points because the modems represented externally connected communications endpoints, terminating at any device within the ESP. URE1 should have identified the gateway devices as electronic access control and monitoring (EACM) devices, which performed the access control, authentication, monitoring, and reporting functions on behalf of the modems. In addition, URE1 failed to identify access points into the ESP for serially connected non-essential Cyber Assets that resided outside of the ESP.

URE1's failure to identify the access points stemmed from a flawed interpretation of a NERC compliance guidance document. URE1 had erroneously determined that Cyber Assets non-essential to

the operation of Critical Assets that were serially connected to Cyber Assets within the ESP did not have to be classified as access points or as being associated with access points.

SERC determined that URE1 was in violation of CIP-005-3a R1.1 because it failed to identify all ESP access points.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 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 failure to identify and designate access points to the ESPs increased the risk of unauthorized access to the implicated ESPs.

Regarding the failure to identify modems as access points, URE1 placed the modems behind secured gateway devices that were providing both access control and authentication functions. As a result, all access attempts arriving at the modems would first have had to pass through the gateway, effectively ensuring that CCAs to which the modems connected were shielded from unauthorized access. Consequently, the failure to identify the modems as access points was an error in documentation.

Regarding the non-routable connections crossing into the ESP, URE1 protected the Cyber Assets that serially communicated with devices inside the ESP within secured facilities or resided inside locked cabinets or cages, and URE1 identified and documented the devices. Additionally, the non-routable nature of the communications technically limited the provision of perimeter protections where such serial communication links are utilized. During the violation, there were no known adverse or negative impacts from not identifying access points for serial (non-routable) connections.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. identify modems as access points for all dial-up accessible facilities;
2. disconnect the modems at several critical facilities;
3. deem one facility not critical through the execution of the risk-based assessment methodology (RBAM);
4. modify its Cyber Asset identification tool to add instructions which would ensure that modems associated with dial-up access are identified as access points;

5. modify its CIP-007 R1 test plan to ensure that modems associated with dial-up access are identified as access points;
6. provide training to the individuals affected by the changes;
7. update ESP diagrams to identify protocol converters as access points;
8. submit Technical Feasibility Exceptions as appropriate for the functions that could not be performed at the access points;
9. update the CIP-007 R1 test procedures to ensure that serial devices connected from outside the ESP have an access point to a device inside the ESP; and
10. provide training for the individuals affected by the procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was completed.

CIP-005-1 R1.1 (SERC2013012498)

SERC sent URE2 an initial notice of a Compliance Audit. Following the notice, URE2 submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.

URE2 failed to identify access points into the ESP for serially connected non-essential Cyber Assets that resided outside of the ESP. URE2 reported that Cyber Assets residing outside of the ESP were serially connected to devices within the ESP and documented, but no access point for the connection was identified.

Within the Critical Assets at issue, URE2 had serial (non-routable) connections from various non-essential Cyber Assets outside of the ESP that connected directly to human-machine interface machines or switches that were identified as CCAs and protected as such. URE2 also had serial connections from non-essential Cyber Assets outside the ESP to protocol convertors that were identified as non-critical Cyber Assets within the ESP and protected as such. The serial connections did not traverse any Cyber Asset boundary device on the ESP that would be considered an access point under CIP-005-1 R1.

URE2's failure to identify the access points stemmed from a flawed interpretation of a NERC compliance guidance document. URE2 had erroneously determined that Cyber Assets non-essential to the operation of Critical Assets that were serially connected to Cyber Assets within the ESP did not have to be classified as access points or as being associated with access points.

SERC determined that URE2 was in violation of CIP-005-1 R1.1 because it failed to identify all ESP access points.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 executed an out-of-cycle RBAM and determined it had no CCAs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify and designate access points to the ESPs increased the risk of unauthorized access to the involved ESPs. However, the Cyber Assets that serially communicated with devices inside the ESP were protected within secured facilities or resided inside locked cabinets or cages, and the devices were identified and documented by URE2. Additionally, the non-routable nature of the communications technically limited the provision of perimeter protections where such serial communication links are utilized. During the violation, there were no known adverse or negative impacts from not identifying access points for serial (non-routable) connections.

URE2's Mitigation Plan to address this violation was submitted to SERC.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE2 certified that the above Mitigation Plan requirements were completed. SERC verified that URE2's Mitigation Plan was complete.

CIP-005-1 R1.5 (SERC2013012488 and SERC2013012496)

SERC sent URE1 and URE2 an initial notice of a Compliance Audit. Following the notice, URE1 and URE2 each submitted a Self-Report to SERC stating that they were in violation of CIP-005-1 R1.5. URE1 and URE2 failed to properly identify certain EACMs and afford certain EACM devices the protective measures specified in CIP-009 R1.

During an internal review, URE1 and URE2 discovered that each had failed to identify network management devices as EACMs based on an incorrect interpretation of the Requirement, despite previously identifying and protecting them as EACMs. SERC determined that several authentication servers included in the Self-Reports were not EACMs and should not have been included.

Additionally, URE1 and URE2 discovered that each had failed to afford other EACMs the protective measures specified in CIP-009 R1. URE1 and URE2 failed to document the steps necessary for the recovery of firewalls within their existing CIP-009 R1 recovery plans.

SERC determined that URE1 and URE2 were in violation of CIP-005-1 R1.5 because each failed to identify properly certain EACM devices and failed to afford certain EACM devices the protective measures specified in CIP-009 R1.

SERC determined the duration of the URE1 violation to be from when the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined the duration of the URE2 violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 implemented an off-cycle RBAM and determined that it does not have any CCAs.

SERC determined that these violations posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to identify properly the management devices as EACMs posed a risk that URE1 and URE2 might not have applied appropriate controls to prevent the theft or modification of authentication credentials or prevent the alteration or disablement of access control rules. Additionally, the failure to include the firewall EACMs in the CIP-009 R1 recovery plan posed a risk that URE1's and URE2's ability to recover the firewall EACMs might be delayed unnecessarily, and thereby impact URE1's and URE2's overall ability to protect and remotely operate its Supervisory Control and Data Acquisition system.

However, regarding the management EACMs, access to the devices was restricted to CIP-authorized personnel and required two-factor authentication. The devices were protected within a secured PSP and resided behind a corporate firewall. No known instances of unauthorized physical or electronic access to the management EACMs occurred during the violation.

Regarding the firewall EACMs, although not part of the CIP-009 R1 recovery plan, recovery plans were available to the technicians that were responsible for the recovery of the firewalls. Moreover, operational recovery of the devices was required on at least two occasions. URE1 and URE2 provided evidence of the device recovery, which indicated they successfully recovered the devices with no undue delay.

URE1's and URE2's Mitigation Plans to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. complete an analysis of its policies, standards, and guidelines for EACMs to determine what controls should be included in distributed enterprise security CIP-003 through CIP-009 procedures;

2. update the relevant procedures, including relevant supporting documentation and references;
3. provide training for individuals affected by the procedural changes;
4. apply controls identified above and prepare evidence to demonstrate compliance with updated procedures; and
5. perform an exercise pursuant to CIP-009 R2 on the updated recovery plans.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE1 and URE2 certified that the above Mitigation Plans requirements were completed. SERC verified that URE1's and URE2's Mitigation Plans were complete.

CIP-005-2 R1.5 (SERC2013011754)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.5.

SERC later determined that the violation began when Version 2 of the CIP Standards became mandatory and enforceable. URE1 failed to ensure that Cyber Assets used in the EACMs of the ESP at its facility were afforded the protective measures specified in CIP-006-2 R3. After the initial discovery of its failure to protect EACMs within a fully enclosed PSP at one facility, URE1 identified additional EACMs residing within a PSP that lacked complete six-wall boundaries at a second facility.

During a review of the PSPs, URE1 discovered three openings greater than 96 square inches under the raised floor below the facility's PSP and nine openings greater than 96 square inches above the false ceiling in a second facility's PSP. The identified openings resulted from URE1's reliance on the erroneous statements of a third-party vendor that it had installed wire mesh in all openings exceeding 96 inches prior to the date of mandatory compliance.

SERC determined that URE1 was in violation of CIP-005-2 R1.5 because it did not afford EACM devices the protective measures specified in CIP-006-2 R3.

SERC determined the duration of the violation from the date the Standard became mandatory and enforceable on URE1 until URE1 closed the openings in the PSPs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to create complete six-wall boundaries protecting EACMs could have allowed

intruders to gain physical access to the EACMs and allowed them to manipulate or destroy the devices. The root cause of the identified violations stemmed from URE1's reliance on the assertions of a third-party consultant. However, the affected PSPs were within existing corporate computer rooms that were restricted to corporate Information Technology personnel. The facilities at issue had on-site physical security staff that monitored the premises 24 hours a day, seven days a week. The EACMs were monitored by an intrusion detection system, which would alert URE1 staff to any unauthorized attempts to interface with the EACMs.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. meet with responsible persons to discuss an appropriate design solution to block the openings;
2. conduct inspections at additional PSPs; URE1 determined that they were properly enclosed by a six-wall border;
3. work with responsible persons to improve the facilities change management process to ensure that the PSPs are appropriately secured from the compliance date forward and further, that changes are not made that compromise PSPs. Specifically, the revised process would ensure that area owners submit a request form to corporate security for approval when establishing a NERC CIP PSP or prior to initiating any changes. This form would trigger a review by corporate security to ensure that proposed plans are consistent with NERC CIP physical security requirements;
4. evaluate vendor proposals based on the design solution and completed work;
5. work with vendors to ensure that all gaps in wire mesh have been corrected with installation of additional wire mesh. Area owners worked with a vendor to seal the heating, ventilating, and air conditioning ducts; and
6. conduct inspections at the remaining PSPs to ensure they are properly enclosed by a six-wall border.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-005-3a R3 (SERC2013012240)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-005-3a R3.

URE1 failed to implement electronic processes for monitoring and logging access at an access point to the ESP 24 hours a day, seven days a week.

During an internal review, URE1 discovered a single ESP access point where it had not enabled access logging for approximately 8% of the configured security policies for that access point. A URE1 firewall analyst had implemented the policies, but failed to configure fully the logging command. The policies represented access permit statements, which were enabled to allow several host machines to communicate with a field data concentrator residing inside an ESP.

SERC determined that URE1 was in violation of CIP-005-3a R3 because it failed to implement electronic processes for monitoring and logging access at an access point to the ESP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from when URE1 implemented the new firewall policies on the facility firewall but failed to enable logging on the firewall policies, until URE1 implemented logging on the firewall policies.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 failed to monitor or log access to an ESP access point that could have left it unable to identify unauthorized access across the ESP access point if the access involved the four policies. Such a situation could have left URE1 unable to analyze any such unauthorized access and respond to prevent similar incursions. However, the policies had been established in accordance with URE1's procedures, including the restriction of access to authorized personnel. All traffic from the host devices was encrypted via a virtual private network tunnel. The failure was limited to a single access point and affected approximately 8% of the security policies established for that access point.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. enable logging on the four policies;
2. update its CIP-005 procedure to institute an independent review process for firewall policy changes; and
3. provide training for individuals affected by the procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.1 (SERC2013011761)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.1. URE1 failed to establish a completely enclosed (six-wall) border for an identified PSP and had not deployed and documented alternative measures to control physical access.

During an internal review, URE1 discovered it did not have a fully enclosed six-wall border at two PSPs. The previously unidentified openings were above false ceilings and were greater than 96 square inches.

In addition, where URE1 could not establish a completely enclosed (six-wall) border around network wiring as required, in two instances URE1 did not deploy and document alternative measures to control physical access to wiring.

SERC determined that URE1 was in violation of CIP-006-1 R1.1 because it failed to establish a completely enclosed (six-wall) border for multiple identified PSPs and had not deployed and documented alternative measures to control physical access.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1's failure to identify openings in PSPs and provide alternative measures of protecting ESP wiring external to a PSP could have allowed an intruder to gain access to CCAs within the PSP or to intercept, manipulate, or degrade ESP communications on the unprotected ESP wiring.

Regarding the first PSP discovery, the unidentified opening was approximately 30 feet above the floor. An intruder would have required rappelling equipment to gain access to the facility and would have entered the room in full view of the operators and any other occupants. The facility was access-controlled and staffed 24 hours a day, seven days a week. The opening was only accessible from an area that had corporate access controls with restricted access.

Regarding the second PSP discovery, the unidentified openings were approximately 30 feet and 20 feet above the floor, respectively. The unsecured openings were within an access-controlled facility that had on-site security staff 24 hours a day, seven days a week. A potential intruder would have to discover the openings above a false ceiling before attempting to gain access to the PSP using those openings.

Regarding the ESP wiring discovery, the ESP wiring in both instances was located within a secured corporate facility that on-site security personnel monitored 24 hours a day, seven days a week. A potential intruder would have to discover the ESP wiring above a false ceiling or below a raised floor before attempting to access it for malicious purposes.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. work with its facilities group to block the openings;
2. work with responsible persons to improve the facilities change management process to ensure that PSPs are appropriately secured from the compliance date forward and that further changes are not made which compromise PSPs. Specifically, the revised process ensures that area owners submit a request form to corporate security for approval when establishing a NERC CIP PSP or prior to initiating any changes to a PSP. This form triggers a review by corporate security to ensure that proposed plans are consistent with NERC CIP physical security requirements;
3. conduct inspections at the remaining PSPs to ensure they were properly enclosed by a six-wall border;
4. re-designate a PSP to include areas where ESP wiring spanned outside the identified PSP;
5. pull armored fiber optic cable to replace the existing fiber wiring which spanned outside the identified PSP;
6. update corporate security processes to include an assessment of network wiring before the creation of a PSP or the re-designation of an existing PSP;
7. provide training for the individuals affected by the revised corporate security process referenced above;
8. review all PSPs to determine which ones require further action to ensure network wiring is being afforded the proper protection pursuant CIP-006 R1.1; and
9. address and bring into compliance any additional issues identified during the review.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (SERC2013012242)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8.

URE1 failed to afford Cyber Assets used in the Physical Access Control Systems for the PSPs the protective measures specified in CIP-007-1 R1, specifically the testing of cybersecurity controls prior to implementing significant changes.

Firstly, URE1 discovered 74 instances where it had not tested PACS cybersecurity controls prior to implementation of significant changes into production. In 22 instances, URE1's test plans only called for testing to ensure the devices still functioned as expected but did not call for testing for any changes to the existing cybersecurity controls. In 17 instances, URE1 failed to implement the cybersecurity controls portion of the existing test plan. In 28 instances, URE1 failed to test any cybersecurity controls on several failover PACS servers because personnel failed to recognize the servers were PACS devices. Finally, there were seven instances where URE1 failed to document that any required testing had been conducted.

Secondly, URE1 failed to afford PACS devices the protective measures specified in CIP-007-1 R3 by failing to assess a security patch for certain PACS components within 30 days of release. URE1 identified a missed assessment of a database security patch. This was the only missed PACS database server patch, and it only applied to two PACS database servers, consisting of a primary server and a standby server.

Thirdly, URE1 discovered a single shared account with read-only access to the PACS was not afforded the protective measures specified in CIP-007-1 R5. This specific account was established on the PACS database server prior to the date of mandatory compliance so that individuals could run nightly reports that were used to manage and review access rights to the URE1 PSPs. Although this shared account was included in quarterly reviews, it was not afforded the protective measures required for shared accounts due to confusion between two teams regarding who was responsible for management of the account.

Finally, URE1 also implemented a change to its PACS production servers without following its documented change management procedures required by CIP-003-3 R6.

The URE1 procedure for change management required all significant changes for PACS to be held out of regular implementation pending a more extensive documented review and testing sessions. In the event that testing in the URE1 quality assurance environment produced negative results,

implementation into production would be halted until resolved. URE1 supplemented the process that described how its personnel would use the change management system to document any requested change to the PACS. URE1 process required the change request to be submitted, reviewed and approved, and tested. URE1 retained all documentation in the change management system.

URE1 applied several patches to all its PACS production servers without following the documented URE1 change management process. These PACS servers controlled all URE1 PSPs.

SERC determined that URE1 was in violation of CIP-006-1 R1.8 because it failed to afford its PACS devices the protections specified in: 1) CIP-007 R1 by failing to adequately or fully test significant changes to PACS devices to ensure there were no adverse effects on existing cybersecurity controls; 2) CIP-007 R3 by failing to assess a security patch for certain PACS components within 30 days of release; 3) CIP-007 R5 by failing to properly manage a shared account for the PACS; and 4) CIP-003 R6 by failing to follow its change management procedures when implementing a change to all its PACS production servers.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a serious or substantial risk. Specifically, the PACS components are essential to maintaining URE1's CCAs in a physically secure state.

Regarding testing, the repeated failure to adequately test changes prior to production deployment, pursuant to CIP-007 R1, increased the risk that the change might result in the inoperability of PACS components as the result of unanticipated file or code corruption or conflicts, and/or the altering of security controls in the environment. Such effects could have made the PACS more susceptible to malicious attacks that could have resulted in the inoperability of PACS components or unauthorized physical access to CCAs. However, the PACS readers would have continued to restrict access based on local memory stored on the readers, even if the PACS servers were disabled.

Regarding the database server patch, URE1's failure to timely assess a security patch pursuant to CIP-007 R3 increased the risk that an attacker could use a vulnerability to compromise the PACS database servers and give access rights to individuals without authorization or disable the PACS database servers. However, the primary facility PSP was manned 24 hours a day, seven days a week, making undetected intrusion into that area difficult. All PSPs had video cameras at the access points, which would allow for identification of any unauthorized intruders. In addition, if the PACS database servers were completely disabled without adding access rights for unauthorized individuals, the door readers and PACS control panels would have relied on internal memory until the databases were restored.

The internal memory would have limited access to those previously authorized for physical access to the PSPs. Finally, the PACS database server was protected behind corporate firewalls.

Regarding the shared account, URE1's failure to secure a shared account with read-only privileges pursuant to CIP-007 R5 increased the risk that unauthorized users might be able to obtain PACS access log information. However, even if the account had been compromised, an attacker would have only been able to obtain PSP access logs in read-only format. The account would not have permitted the modification of any PACS permissions or component operations. In addition, URE1 implemented a solution that required two-factor authentication for PACS system access.

Regarding the change management procedures, URE1's failure to follow the change management procedures pursuant to CIP-003 R6 could have resulted in the degradation of cybersecurity controls because of the installation of unapproved and untested patches. However, the patches had been assessed, tested, and approved for deployment on the corporate network and had also been assessed and approved for the additional testing required before they could be deployed to the PACS devices. The patches were in place for less than 14 days before discovery. The untested patches had been tested and deployed in non-critical systems without incident. Subsequent testing found that the untested and deployed patches did not affect the existing cybersecurity controls on the PACS.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. develop a new PACS test plan that will replace the existing PACS test plan. The new PACS test plan clearly identified the steps required to ensure changes to the PACS system do not adversely affect existing cybersecurity controls;
2. conduct training session with testing team members on the new PACS test plan;
3. execute the new PACS test plan against the production baseline and remediate any new potential violations discovered. If any were discovered, an email notification would be sent to SERC;
4. revise its CIP-007-3 R3 procedure as required by CIP-006-3 R2.2 to accurately document the processes supporting security patch management for the PACS;
5. provide training for individuals affected by the CIP-007 R3 procedural change;
6. assess missing security patch;
7. change the PACS shared database password;

8. revise its CIP-007 R5 procedure to include a process for coordinating the quarterly review of all accounts with access to the PACS;
9. provide training for individuals affected by the CIP-007 R5 procedural changes;
10. revoke the shared account access from the PACS environment;
11. apply patches in question to the PACS quality assurance servers and test;
12. provide training to the patching administration group to raise awareness that in the event technical issues occur, all patching of PACS servers would be halted until technical issues are resolved;
13. determine potential sources of failure in PACS change control and configuration management processes; and
14. develop and implement an action plan based on the results of the analysis of potential sources of failure.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-006-1 R1.8 (SERC2013012244)

SERC sent URE2 an initial notice of a Compliance Audit. Following the notice, URE2 submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8.

URE2 failed to afford Cyber Assets used in the PACS for the PSPs the protective measures specified in CIP-007-1 R1, specifically the testing of cybersecurity controls prior to implementing significant changes.

URE2 discovered 64 instances where PACS cybersecurity controls were not tested prior to implementation into production. There were 22 instances where URE2's test plans called for testing to ensure the devices still functioned as expected but did not call for testing for any changes to the existing cybersecurity controls. There were nine instances where URE2 failed to implement the cybersecurity controls portion of the existing test plan. There were 28 instances where URE2 failed to test any cybersecurity controls on several failover PACS servers because personnel failed to recognize the servers were PACS devices. Finally, there were five instances where URE2 failed to document that any required testing had been conducted.

In addition, URE2 failed to afford PACS devices the protective measures specified in CIP-007-1 R3 by failing to assess a security patch for certain PACS components within 30 days of release. URE2 identified a missed assessment of a database security patch that was released. This was the only missed PACS database server patch, and it only applied to two PACS database servers, consisting of a primary server and a standby server.

Finally, URE2 discovered a single shared account with read-only access to the PACS that was not afforded the protective measures specified in CIP-007-1 R5. This specific account was established on the PACS database prior to the date of mandatory compliance so that individuals could run nightly reports that were used to manage and review access rights to the URE2 PSPs. Although this shared account was included in quarterly reviews, it was not afforded the protective measures required for shared accounts due to confusion between two teams regarding who was responsible for management of the account.

SERC determined that URE2 was in violation of CIP-006-1 R1.8 because it failed to afford its PACS devices the protections specified in: 1) CIP-007-1 R1 by failing to adequately or fully test significant changes to PACS devices to ensure there were no adverse effects on existing cybersecurity controls; 2) CIP-007 R3 by failing to assess a security patch for certain PACS components within 30 days of release; and 3) CIP-007 R5 by failing to properly manage a shared account for the PACS.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE2 until URE2 executed an out-of-cycle RBAM and determined it had no CCAs.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, the PACS components are essential to maintaining URE2's CCAs in a physically secure state.

Regarding testing, the repeated failure to adequately test changes prior to production deployment pursuant to CIP-007 R1 increased the risk that the change might result in the inoperability of PACS components as the result of unanticipated file or code corruption or conflicts and/or the altering of security controls in the environment. Such effects could have made the PACS more susceptible to malicious attacks that could have resulted in the inoperability of PACS components or unauthorized physical access to CCAs. However, the PACS readers would have continued to restrict access based on local memory stored on the readers, even if the PACS servers were disabled.

Regarding the database server patch, the failure to timely assess a security patch pursuant to CIP-007 R3 increased the risk that an attacker could have used a vulnerability to compromise the PACS database servers. The compromise of PACS database servers could have given access rights to

individuals without authorization or allowed individuals the ability to disable the PACS database servers. However, all PSPs had video cameras at the access points, which would have allowed for identification of any unauthorized intruder. In addition, if the PACS database servers were completely disabled without adding access rights for unauthorized individuals. The door readers and PACS control panels would have relied on internal memory until the databases were restored, which would limit access to those previously authorized for physical access to the PSPs. Finally, the PACS database server was protected behind corporate firewalls.

Regarding the shared account, the failure to secure a shared account with read-only privileges pursuant to CIP-007 R5 increased the risk that unauthorized users might be able to obtain PACS access log information. However, even if the account had been compromised, an attacker would only be able to obtain PSP access logs in read-only format. The account would not have permitted the modification of any PACS permissions or component operations. In addition, URE2 implemented a solution that required two-factor authentication for PACS system access.

URE2's Mitigation Plan to address this violation was submitted to SERC.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE2 certified that the above Mitigation Plan requirements were completed. SERC verified that URE2's Mitigation Plan was complete.

CIP-006-1 R3 (SERC2013012490 and SERC2013012495)

SERC sent the UREs an initial notice of a Compliance Audit. Following the notice, URE1 and URE2 submitted Self-Reports to SERC stating that each was in violation of CIP-006-1 R3.

Both entities had failed to retain evidence to demonstrate that they had implemented immediate human observation of PSP access points during PACS or communication outages.

The UREs' procedures required security personnel to notify the Critical Asset owner where an affected PSP existed of planned or unplanned outages of the PACS or the PACS communications network. The procedure also stated that the Critical Asset owner would be responsible for monitoring and controlling access of all authorized and unauthorized personnel.

URE1 had 365 unplanned communication outages that lasted between 15 minutes and three hours, 22 communication outages that lasted between three to six hours, 26 communication outages that lasted

between six and 24 hours, and three communication outages that lasted more than 24 hours. All the unplanned outages were due to various technical issues resulting from service provider issues or weather events.

URE2 had 84 unplanned communication outages that lasted between 15 minutes and three hours, 13 unplanned communication outages that lasted between three to six hours, ten unplanned communication outages that lasted between six and 24 hours, and three unplanned communication outages that lasted more than 24 hours. All the unplanned outages were due to various technical issues resulting from service provider issues or weather events.

Combined, the entities had planned 13 PACS server outages, for server updates, that lasted between 15 minutes and three hours.

All outages were documented by security. Planned outages were documented as change order tickets, and unplanned outages were documented in a manual communication error log. Security also maintained a manual call log to document the call to the Critical Asset owner regarding the PACS outages.

However, neither URE1 nor URE2 was able to provide any evidence that demonstrated that the manual monitoring occurred when the Critical Asset owner was notified of planned or unplanned outages. This was due to the entities' failure to define adequately the meaning of "immediate" review in procedural documentation. Further, the entities failed to relay clearly the necessity of an "immediate" response to personnel responsible for monitoring the physical access points in the event of an outage of automated controls.

SERC determined that URE1 and URE2 were in violation of CIP-006-1 R3 because they failed to retain evidence to demonstrate that they had implemented human observation of PSP access points during PACS or communication outages.

SERC determined the duration of the violations to be from the date the Standard became mandatory and enforceable on URE1 and URE2 until URE1 completed its Mitigation Plan, and until URE2 removed all remote routable protocols to its Critical Assets leaving them with no CCAs.

SERC determined that these violations posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the UREs' failure to review unauthorized access attempts immediately could have allowed an unauthorized individual to gain access undetected during an outage, and not be detected until the outage concluded. However, the UREs supplied evidence to demonstrate that both planned and unplanned outages had been logged, and that facility managers of

the impacted PSPs were contacted regarding the outage. CCAs contained within the PSP affected by the PACS outage were protected by an intrusion detection system that was configured to alert the UREs' personnel to any unauthorized electronic access attempts occurring locally at the implicated machine.

URE1's and URE2's Mitigation Plans to address these violations were submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. define "immediate" and document the approach to ensure unauthorized access attempts are immediately assessed during PACS or communication outages;
2. revise the corporate physical security procedure to document sufficient technical and procedural controls to immediately review unauthorized access attempts during PACS or communication outages; and
3. implement and communicate procedural changes to personnel responsible for implementing the revised corporate security physical security procedure.

URE2's Mitigation Plan required URE2 to execute an off-cycle RBAM, which resulted in a determination that URE2 does not have any CCAs.

URE1 and URE2 certified that the above Mitigation Plans requirements were completed. SERC verified that URE1's and URE2's Mitigation Plans were complete.

CIP-006-3c R5 (SERC2013011763)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-006-3c R5. URE1 failed to review immediately an unauthorized access attempt alarm on one of its PSPs.

The URE1 security console received a "door open too long" alarm annunciator for a secured door at one facility. The security officer on duty acknowledged this alarm, but the security officer failed to follow URE1's procedures and did not respond or facilitate a response immediately to investigate the cause of the alarm. Approximately four hours later, an employee noticed the door at issue was open slightly and immediately left a voice message for the compliance program manager. This employee also assessed the door to determine why it was not closing and made the necessary repairs in order to get the door functioning properly and re-secured.

The compliance program manager returned to the office and received the message from the employee who discovered the door issue and repaired it. The compliance program manager notified corporate security, which investigated and determined, through review of the video footage, that there were no unauthorized access attempts during the approximately 4 hours that the door was damaged and unsecured.

SERC determined that URE1 was in violation of CIP-006-3c R5 because it failed to review immediately an unauthorized access attempt alarm received from the alarm on one of its PSPs.

SERC determined the duration of the violation to be from when URE1 corporate security received a door alarm for the facility and failed to respond immediately, through when a URE1 employee secured the door.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The failure to investigate the alarm immediately could have allowed an intruder to gain physical access to CCAs for an extended period without being challenged, potentially giving an intruder time to manipulate or destroy CCAs.

The potential risk of the violation was mitigated by several factors. The PSP door at the facility is in a cardkey access-controlled area, which is within an access-controlled building that is manned 24 hours a day, seven days a week by onsite security personnel. The PSP door is monitored by closed circuit television cameras, which are recorded for investigative purposes. Review of the video found no attempts at unauthorized access during the violation. Lastly, the Cyber Assets contained within the PSP had an intrusion detection system running to alert URE1 personnel to any unauthorized electronic access attempts on the devices, in the case that an intruder attempted to log-on to a device from inside the PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. secure the bolt on the automatic door;
2. terminate the security officer on duty;
3. ensure the understanding of the policy and procedure between the manager of the security team and the supervisor of the security team through a meeting with the security team to discuss areas of concern; and

4. create a NERC/Regulated desk in the new security team. This desk would focus on creating and delivering comprehensive training to security team staff, managing and responding to all access control issues at NERC CIP sites, and ensuring a clear understanding of security team operating processes and procedures.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R1 (SERC2013012486)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R1.

URE1 had procedures that lacked sufficient detail to ensure significant changes to existing Cyber Assets within the ESP did not affect existing cybersecurity controls.

During an internal assessment, URE1 identified a deficiency in its testing procedures. Although the URE1 procedures called for testing to occur whenever there was a security patch deployed, the procedures did not address changes to software, version upgrades, or new applications. The procedural guidance focused primarily on the review of ports and services specifically after a security patch deployment. URE1 also omitted testing of significant changes to ensure that those changes did not affect existing cybersecurity controls such as malware prevention software, account management, and security status monitoring. Lastly, the procedure did not specify how testing results should be documented.

SERC determined that URE1 was in violation of CIP-007-1 R1 because it failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 conducted cybersecurity controls testing on each affected Cyber Asset.

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, URE1's failure to test security controls after significant changes could have permitted implemented changes to eliminate or degrade existing security controls and permit unauthorized access to CCAs, resulting in available attack vectors to CCAs, which could have permitted compromise of the CCAs.

However, URE1 did ensure that significant changes did not change the enabled ports and services. In addition, all Cyber Assets were secured within ESPs and PSPs, and the ESPs were protected by an intrusion prevention system.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. review its guidelines for test procedures and develop a list of controls to be tested by asset type;
2. update a test procedure to include a comprehensive list of cybersecurity controls;
3. update a test procedure to ensure the test results are documented for each significant change;
4. provide training for the individuals affected by the procedural changes made to the test procedure; and
5. perform a cybersecurity controls test on each of the managed Cyber Asset types.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R2.2 (SERC2013012487)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R2. URE1 failed to implement sufficiently its process to ensure that only those ports and services required for normal and emergency operations were enabled.

While conducting an internal compliance review, URE1 discovered that there were ports and services enabled on multiple CCAs and non-critical Cyber Assets within the ESP that were not documented as being required for normal or emergency operations.

Approximately 15% of the Cyber Assets had several hundred ports and services that were enabled but without supporting documentation for why the ports and services were required. URE1 had identified undefined ports and services as action items to address in its annual CVAs, but due to deficiencies in its ports and services procedure, these ports and services were not disabled or documented as being necessary for normal or emergency operations. URE1 concluded the root cause of the violation was a human performance issue where support personnel failed to take the remedial actions required in its

systems security management procedure to disable unused ports and services where necessary and document the results.

SERC determined that URE1 was in violation of CIP-007-1 R2.2 because it failed to disable ports and services not required for normal and emergency operation.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 documented the need for the enabled ports and services required for normal or emergency operations and disabled the ports and services that were not required for normal or emergency operations.

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE1's failure to document the need for enabled ports and services and its failure to disable unneeded ports and services for over several years gave individuals a protracted opportunity to exploit or degrade CCAs, and potentially cause URE1 to lose its visibility of, or control over, its portion of the BPS. Moreover, the failure of URE1 to remediate the port and service issues identified during its annual CVAs is indicative of further weaknesses in URE1's documentation and justification of ports and services that were enabled. However, CCAs and non-critical Cyber Assets were secured within an established ESP, which included an intrusion prevention system.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. conduct a review session for the relevant group on the CIP-007 R2 procedure;
2. review and document the justification of the "not defined" or "unknown" ports and services;
3. disable any unnecessary ports and services;
4. review and evaluate the CIP-007 R2 procedure to determine if any process changes were required and update the CIP-007 R2 procedure; and
5. provide training for the individuals affected by the procedural changes to the CIP-007 R2 procedures.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R3 (SERC2013012532)

URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R3. URE1 failed to review applicable software security patches for all Cyber Assets within the ESP within 30 days of availability and failed to document adequately the assessment and implementation of security patches.

SERC determined that URE1 was in violation of CIP-007-1 R3 because it failed to review applicable software security patches for all Cyber Assets within the ESP within 30 days of availability and failed to document adequately the assessment and implementation of security patches. The associated Cyber Assets included communication processors, EMS devices, workstations, and servers.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable for URE1 until URE1 implemented an interim solution for tracking the implementation of security patches.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the failure to document adequately the application of security patches or the decision not to apply security patches where appropriate increased the risk that URE1 may have failed to identify patching gaps. Additionally, the failure to timely assess patches affected various CCAs and non-critical Cyber Assets and increased the time those Cyber Assets were exposed to vulnerabilities. These failures could allow a malicious actor to use previously identified vulnerabilities to disrupt URE1's ability to monitor and control its portion of the BPS.

However, the communication processors were isolated to communications originating within the URE1 EMS, and they were located in physically secured facility environments. Regarding the EMS devices, the EMS ESPs were monitored by network-based intrusion prevention. The workstations were deployed with host-based intrusion detection systems. One patch affected seven Cyber Assets and a second patch was assessed three days past the permitted 30-day assessment window. In addition, the ESP network was segregated from the enterprise network. The URE1 EMS had its own active directory that is separate from the enterprise active directory. All of the Cyber Assets involved in this violation are secured within an established ESP and PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. create a requirements list from all the groups involved in the patch management process to ensure the implementation of security patches or upgrades were sufficiently documented;

2. implement an interim solution for tracking the implementation of patches;
3. implement the interim solution as a permanent solution for tracking the implementation of changes, and then document and communicate procedural changes in support of the permanent solution;
4. apply all applicable security patches for the missed assessments;
5. complete and document all applicable patch assessments for the specific product;
6. update the CIP-007 R3 procedure to require the assessor to review their software inventory for any manual patch discovery processes. Reviewing the software inventory as part of the discovery process ensures that all security patch alerts or advisories are tracked and assessed for all applicable software versions;
7. provide training for the individuals affected by the updated CIP-007 R3 procedure;
8. update the CIP-007 R1 procedure to address steps for adding, incrementing, or removing software versions to the patch assessment process;
9. provide training for the individuals affected by the updated CIP-007 R1 procedure;
10. remap all instances of the affected software application to correct entries with a third-party vendor, which was monitoring a different version of the software;
11. assess patches missed due to vendor configuration error;
12. coordinate with the third-party vendor to look for other instances of incorrect associations or dead links;
13. assess patches missed due to the systems failure;
14. install monitoring and notifications to alert on failed application conditions relating to the task creation and initial email notification functions;
15. survey industry peers to look for patch management best practices that could be applied;
16. perform a review of all automated functions of the patch management alerting process and ensure system personnel are promptly notified of the failure of any function that could impact compliance;
17. analyze all potential patch management sources of failure across all accountable groups; and
18. if necessary, execute an action plan to address new potential sources of failure or best practices not previously addressed.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R6 (SERC2013012243)

SERC sent URE1 a notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R6.

URE1 failed to implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the ESP.

URE1's procedure for security monitoring required URE1 to monitor CCAs for attempts to connect to unauthorized ports and services, however the procedure lacked sufficient detail to meet the requirements of CIP-007 R6.

URE1 also did not proactively review its system for potential Cyber Security Incidents or events related to cybersecurity that might not produce functional abnormalities. Instead, URE1 operationally depended on the system operators and their experience and knowledge to detect and alert system administrators of any functional abnormalities.

SERC determined that URE1 was in violation of CIP-007-1 R6 because it failed to implement automated tools or organizational process controls to monitor system events that are related to cybersecurity.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 implemented an automated process to monitor and alert on system events related to cybersecurity.

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, URE1's failure to monitor for events related to cybersecurity could have permitted a malicious actor to gain access to or compromise CCAs, thereby threatening URE1's visibility over, or control of, its portion of the BPS. However, URE1 had trained system operators on shift 24 hours a day, seven days a week who monitored the system for system performance issues. URE1 utilized an intrusion prevention system within the secured ESPs. All involved CCAs were secured within an ESP and PSP.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. implement a security information and event management (SIEM) system to monitor and alert on system events related to cybersecurity for Cyber Assets within the ESPs;
2. update CIP-007 R6 procedure to reflect the new SIEM system and specify and require documentation necessary to demonstrate compliance with CIP-007 R6;
3. provide training to individuals affected by CIP-007 R6 procedural changes;
4. update change management procedures to ensure all Cyber Assets are communicating with the SIEM system, where technically feasible; and
5. provide training to individuals affected by change management procedural changes.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-007-1 R8.3 (SERC2013012489)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R8.3.

URE1 failed to have sufficient detail in its internal procedures to ensure its staff adequately performed a review of the controls for default accounts during CVAs.

URE1's CVA procedure required the annual review of default accounts, evaluation of the results, and that the remediation plan for any issues discovered be documented and tracked through completion.

Through an internal assessment of its CVA procedure, URE1 determined that the existing CVA procedure, although requiring the review of all default accounts, did not contain adequate detail on how to conduct a review of controls for default accounts.

URE1's CVA remediation plans documented that a scan for default applications and system accounts and log-ins was conducted for a period of two years. The remediation plans also documented that the scan found no default accounts enabled. URE1's CVA remediation plan for the following year did not document that a scan for default user accounts had been conducted.

URE1 reviewed the CVA procedures for all other areas and found no other deficient CVA processes.

SERC determined that URE1 was in violation of CIP-007-1 R8.3 because it failed to have sufficient detail to perform an adequate review of the controls for default accounts. The existing procedure did not address the controls associated with default accounts.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE1 until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE1's failure to establish sufficient procedures to ensure adequate evaluation and controls around default accounts during annual CVAs could have permitted a malicious individual to exploit an existing default account, gain access and control of CCAs, and eliminate or corrupt data being used to make operational decisions. However, URE1 did include a review of enabled ports and services in its annual CVAs and had documented action plans to remediate any issues that were discovered during the CVAs. All Cyber Assets were secured with an ESP and a PSP, and the network was monitored via network- and host-based intrusion detection systems. Security status monitoring of Cyber Assets within the ESP indicated no unauthorized or malicious activity during the violation.

URE1's Mitigation Plan to address this violation was submitted to SERC.

URE1's Mitigation Plan required URE1 to:

1. update its CIP-007 R8.3 procedure to include all controls for default accounts;
2. provide training for the individuals affected by the procedural changes made to the CIP-007 R8.3 procedure;
3. obtain asset access control lists to review the population of default accounts and their available controls; and
4. execute updated CIP-007 R8.3 procedure to include a review of all default accounts and their controls.

URE1 certified that the above Mitigation Plan requirements were completed. SERC verified that URE1's Mitigation Plan was complete.

CIP-009-1 R1 (SERC2013012491)

SERC sent URE1 an initial notice of a Compliance Audit. Following the notice, URE1 submitted a Self-Report to SERC stating that it was in violation of CIP-009-1 R1. URE1's recovery procedures lacked sufficient detail to recover all CCAs.

URE1 implemented two separate recovery plans for its CCAs. The separate plans addressed CCAs associated with different groups.

URE1 completed an internal review of the first plan. It discovered that the existing recovery procedures were insufficient to ensure a complete recovery from the loss of CCAs. SERC reviewed the first plan and determined that it did not provide details on how to manage properly hardware changes or upgrades resulting from a recovery, and it failed to define roles and responsibilities of responders and response actions to events of varying duration and severity. URE1 maintained a supplemental document detailing the required steps for documenting, testing, and updating hardware changes, but this hardware change procedure was not linked to or referenced from the first plan.

Regarding the second plan, SERC determined that it was written as a higher-level disaster recovery plan of facilities and systems, and failed to address the recovery of the specific Cyber Assets in service within the second group, define the roles and responsibilities of responders, and specify the required actions in response to events of varying severity and duration. Nevertheless, the second plan was supplemented by a recovery process document that addressed the replacement of CCAs and provided instructions to recover Cyber Assets and return them to service using previously approved settings. The recovery process document also referenced a site where a replacement Cyber Asset could be obtained, but did not provide any detail on the systems or tools and applications that should be used to recover the replacement Cyber Asset to return to normal operations.

SERC determined that URE1 was in violation of CIP-009-1 R1 because its recovery procedures lacked sufficient detail to recover all CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable until URE1 completed its Mitigation Plan.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE1 successfully recovered CCAs throughout the violation period without issues, depending on the skill and experience of the technicians and system operators. URE1 conducted successful weekly failover of the systems to back-up redundant systems, which would have been available in the event of a prolonged recovery of a CCA, or in the event of a more widespread event

affecting multiple CCAs. The response personnel for URE1 were trained and aware of the existing procedures and were able to respond to and recover CCAs based on their experience and knowledge.

URE1's Mitigation Plan to address this violation was submitted to SERC. URE1's Mitigation Plan required URE1 to:

For The First Plan

1. assess the CIP-009 procedures and evaluate the steps to properly perform a technical recovery of each CCA type;
2. update the CIP-009 procedures incorporating changes based on the assessments completed for each CCA type;
3. approve and distribute updated CIP-009 procedures;

For The Second Plan

4. review and enumerate the Cyber Asset types which needed additional details added to the existing CIP-009 technical recovery procedure;
5. create a schedule to update procedures based on the list of Cyber Asset types that needed additional details added to the CIP-009 recovery procedures;
6. update procedures for half of the Cyber Asset types based on the schedule previously developed; and
7. complete procedure updates for the remaining Cyber Asset types.

URE1 certified that the above Mitigation Plan requirements were completed.

SERC verified that URE1's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of one hundred twenty thousand dollars ($120,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE1 and URE2 had prior violation history, which was considered as an aggravating factor in the penalty determination;
2. the UREs had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor;

3. URE1 self-reported the violation of CIP-003-3 R6. The UREs did not receive mitigating credit for self-reporting the remaining violations because the Self-Reports were submitted after receiving notice of an upcoming Compliance Audit;
4. the UREs were cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of SERC2013012483, SERC2014013371, SERC2013012237, SERC2013011770, SERC2013012498, SERC2013012488, SERC2013012496, SERC2013011754, SERC2013012240, SERC2013011761, SERC2013012490, SERC2013012495, SERC2013011763, SERC2013012486, SERC2013012532, SERC2013012243, SERC2013012489, and SERC2013012491 posed a minimal or moderate risk. The violations of SERC2013012242, SERC2013012244, and SERC2013012487 posed a serious or substantial risk to the reliability of the BPS, as discussed above;
7. as explained in more detail in Attachment A to the Settlement Agreement, in addition to paying the monetary penalty, the UREs has completed or has committed to complete the following above-and-beyond mitigating actions, which SERC took into consideration when assessing the proposed penalty:
    a. UREs have hired additional full-time staff resources and converted some contractors to permanent positions, with some of the additional personnel dedicated to NERC CIP compliance and activities focused on the UREs' CIP Version 5 implementation. Although the remaining additional personnel are not dedicated compliance resources, the UREs report that the extra staff has allowed existing compliance resources to focus more time on improving their controls and accurately executing existing compliance processes.
    b. UREs have provided NERC CIP personnel with basic human performance training and personnel with advanced human performance training. UREs also provided personnel with root cause analysis training to support cause identification with all future Self-Report efforts. The cost of this training was approximately $50,000.
    c. UREs have implemented firewall analyzer software that actively monitors UREs' firewalls protected pursuant to the CIP Standards. Implementation of the firewall analyzer software cost approximately $485,000.
    d. UREs have conducted other mitigation efforts outside of its formal Mitigation Plans for CIP-004 R4, CIP-006-3 R2.2, CIP-006-3 R5, CIP-007 R1, and CIP-007 R3 that SERC considered to be mitigating factors in the penalty determination.
8. 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 twenty thousand dollars ($120,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[4]

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,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 18, 2014 and approved 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred twenty thousand dollars ($120,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Attachments to be Included as Part of this Notice of Penalty

REDACTED FROM THIS PUBLIC VERSION

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

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

*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.	Marisa A. Sifontes* General Counsel Drew R. Slabaugh* Legal Counsel Rebecca A. Lindensmith* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 414-5244 (704) 414-5230 (704) 357-7914 – facsimile msifontes@serc1.org dslabaugh@serc1.org rlindensmith@serc1.org James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Andrea B. Koch* Director of Compliance and Analytics SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org

Conclusion

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

Respectfully submitted,

/s/ Edwin G. Kichline

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

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

Sonia C. Mendonça
Associate General Counsel and Senior
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

cc: Unidentified Registered Entities
SERC Reliability Corporation

Attachments