December 30, 2013

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

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

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXXX, 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-004-1 R2 and R4; CIP-004-3 R2 and R4; CIP-005-1 R1; CIP-005-1 R1, R2, and R4; CIP-006-1 R1; CIP -006-3c R2; and CIP-007-1 R1, R2, R3, R5, and R8. According to the Settlement Agreement, URE neither admits nor denies the violations, but has 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 identified as NERC Violation Tracking Identification Numbers SERC200900284, SERC201000551, SERC201000552,

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2013). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation.

SERC201000586, SERC201100776, SERC2011007429, SERC2011007639, SERC2011007985, SERC2011007986, SERC2011007987, SERC2011007988, SERC2011007989, SERC2011007990, SERC2011007992, SERC2011007993, SERC2012010331, SERC2012011169, SERC2013012004, and SERC2013012236 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

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

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	URE	NOC-2226	SERC200900284	CIP-004-1	R4	Lower	$120,000
			SERC201000551	CIP-004-1	R2; R2.1	Medium	
			SERC201000552	CIP-004-1	R4; R4.1	Lower	
			SERC201000586	CIP-007-1	R5; R5.2.1	Medium	
			SERC201100776	CIP-004-3	R4; R4.2	Lower	
			SERC2011007429	CIP-005-1	R1; R1.4	Medium	
			SERC2011007639	CIP-007-1	R5; R5.2	Lower	
			SERC2011007985	CIP-004-3	R4	Lower	

			SERC2011007986	CIP-005-1	R1; R1.1; R1.5	Medium	
			SERC2011007987	CIP-005-1	R2; R2.2	Medium	
			SERC2011007988	CIP-005-1	R4; R4.2	Medium	
			SERC2011007989	CIP-006-1	R1; R1.7; R1.8	Medium	
			SERC2011007990	CIP-007-1	R2; R2.2	Medium	
			SERC2011007992	CIP-007-1	R8; R8.3	Medium	
			SERC2011007993	CIP-007-1	R1	Medium	
			SERC2012010331	CIP-006-3c	R2; R2.2	Medium	
			SERC2012011169	CIP-004-3	R2; R2.1	Medium	
			SERC2013012004	CIP-006-3c	R1; R1.6	Medium	
			SERC2013012236	CIP-007-1	R3	Lower	

CIP-004-1 R4 (SERC200900284)

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

CIP-004-1 R4 provides:

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

R4.1. The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

R4.2. The Responsible Entity shall revoke such access to Critical Cyber Assets within 24 hours for personnel terminated for cause and within seven calendar days for personnel who no longer require such access to Critical Cyber Assets.

CIP-004-1 R4 has a "Lower" Violation Risk Factor (VRF) and a "Lower" Violation Severity Level (VSL).

URE submitted a Self-Report to SERC stating that it failed to maintain an accurate list of personnel with authorized unescorted physical access to Critical Cyber Assets (CCAs) and it failed to revoke unescorted physical access to CCAs within seven calendar days for personnel who no longer required such access, in violation of CIP-004-1 R4.

URE submitted additional Self-Reports stating that it was in violation of CIP-004-1 R4. SERC determined that these Self-Reports were related to the first Self-Report, which involved the same Standard and Requirement, and decided to treat the subsequent Self-Reports as an expansion of the scope of the violation.

SERC determined that URE failed to comply with the requirements of CIP-004-1 R4 for several individuals, all of whom had authorized unescorted physical access rights to CCAs. Specifically, URE failed to revoke access and update its access list within seven days for approximately half of the individuals and failed to update its access list within seven days for approximately one-third of the individuals. In addition, URE mistakenly granted access when it was neither requested nor required for approximately one-sixth of the individuals. This violation involved approximately one percent of individuals with unescorted physical access to CCAs.

URE confirmed through a review of its Physical Security Perimeter (PSP) access logs that one individual involved entered a PSP four times after access should have been revoked.

SERC determined that URE had a violation of CIP-004-1 R4 for failing to comply with the requirements of CIP-004-1 R4 with respect to the individuals involved, all of whom had authorized unescorted physical access rights to CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE updated its access list for the last individual.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE confirmed through a review of PSP logs that all but one of the individuals who retained physical access to CCAs or remained on URE's access list made no attempt to access URE's CCAs after their access rights were revoked or should have been revoked. The remaining individual was an URE employee who entered a PSP that was continuously manned. Each of the 13 individuals involved was in good standing with URE prior to and after this violation.

CIP-004-1 R2.1 (SERC201000551)

CIP-004-1 R2 provides in pertinent part:

> R2. The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.
>
> R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

***

CIP-004-1 R2.1 has a "Medium VRF and a "Severe" VSL.

During a Spot Check (Spot Check), SERC discovered that URE failed to produce evidence that two individuals had completed cyber security training within 90 days of being granted access to CCAs, a violation of CIP-004-1 R2.1.

In the first case, URE provided cyber security training to an individual 91 days after granting the individual access to CCAs. In the second case, URE granted an individual access to CCAs, and then revoked that access before 90 days had passed, but failed to provide cyber security training. The second individual remained with URE and was granted access to CCAs at a later date, after completing the cyber security training.

URE later submitted a Self-Report to SERC stating that it found additional personnel who had been granted access to CCAs but did not complete the required training within 90 days of being granted

access. SERC determined that the Self-Report was related to the Spot Check finding and decided to treat the subsequent Self-Report as an expansion of the scope of the violation.

In total, URE granted several dozen contractors and employees access to CCAs but did not ensure that these individuals completed cyber security training within 90 days of being granted access. Of these individuals, approximately two-thirds received the cyber security training after 90 days had passed and approximately one-third never received the cyber security training before URE revoked their access. This violation involved approximately five percent of individuals with authorized access to CCAs.

SERC determined that URE had a violation of CIP-004-1 R2.1 for failing to ensure that all personnel having access to CCAs were trained within 90 calendar days of being granted access.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All the individuals were in good standing with URE prior to and after this incident. Of the individuals who did not receive cyber security training within 90 days, all but three had PRAs conducted without incident within 30 days of being granted access. The remaining three individuals had their access revoked before 30 days passed.

CIP-004-1 R4.1 (SERC201000552)

CIP-004-1 R4 provides in pertinent part:

> R4. 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.
>
> ***

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

During the Spot Check, URE failed to provide evidence that it conducted a quarterly review of its lists of personnel with access to CCAs. URE used two active directory (AD) groups to control the access rights of personnel with authorized cyber or authorized unescorted physical access to CCAs. One AD group covered normal employees with a need for access to CCAs and the second AD group covered technical/engineering personnel. Both AD groups included the specific access rights of the individuals, whether that involved only cyber access, only physical access, or both cyber and physical access.

URE also had a separate established physical access list. In practice, URE added all personnel with cyber access to the physical access list, even if they had no physical access rights under the AD groups. This practice allowed URE to maintain a single list of all personnel with authorized access to CCAs on the established physical access list, but the resulting physical access list did not accurately specify the true access rights of all personnel. URE reviewed this physical access list on a seven-day cycle and used it to flag and manage changes in personnel, changes in access rights, and the revocation of access. However, URE failed to conduct quarterly reviews of its AD groups, which had the specific access rights of all URE personnel.

URE submitted a Self-Report to SERC stating that it granted physical access to CCAs to three individuals in error and failed to perform Personnel Risk Assessments (PRAs) on them. SERC further determined that the Self-Report was directly related to the Spot Check finding, which involved the same Standard and Requirement, and decided to treat the Self-Report as an expansion of the scope of the violation.

Specifically, URE inadvertently granted three individuals authorized unescorted physical access to CCAs who did not need such access and did not request it. Each individual was granted access for less than 30 days before URE revoked the access. URE failed to include any of these individuals on its list of personnel with authorized cyber or authorized unescorted physical access to CCAs. All three individuals did not know that they had been granted access to CCAs, and none used or attempted to use their access.

SERC determined that URE had a violation of CIP-004-1 R4.1 for failing to review the lists of its personnel with authorized cyber or authorized unescorted physical access to CCAs on a quarterly basis and for granting authorized unescorted physical access to CCAs to personnel who did not need such access or request it.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had AD group lists that specified the individual access rights of its personnel. All of the personnel with authorized access involved in the AD group instance possessed valid PRAs and were current with their CIP training. The three personnel granted access in error in the second instance were not aware that they had access and did not attempt to use their access during the period of the violation. URE revoked the access of these individuals within 30 days.

CIP-007-1 R5.2.1 (SERC201000586)

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

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> ***
>
> R5.2. 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.
>
> ***

CIP-007-1 R5.2.1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it discovered several CCAs, specifically terminal servers, that contained default accounts that had not been renamed, disabled, removed, or had the password changed. URE discovered this issue after its annual Cyber Vulnerability Assessment (CVA).

SERC determined that URE had a procedure that addressed the disabling of system default accounts and required that default system accounts be removed from Cyber Assets. Although this procedure was in place at the time this violation occurred, URE did not utilize this procedure for the terminal servers because it was unaware of the default username and password associated with the terminal servers. The terminal servers could only be accessed through forefront endpoint protection (FEP) servers, to which five to fifteen personnel had access.

After discovering this issue, URE learned that its energy management system (EMS) vendor was also unaware of the existence of default accounts on the terminal servers. As a result, the vendor did not provide URE with any information or documentation that these default accounts were present prior to URE's discovery of their existence.

SERC determined that URE had a violation of CIP-007-1 R5.2.1 for failing to remove, disable, rename, or change the password for the default system accounts on eight CCAs before placing them into service.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE changed the password for the default accounts on the CCAs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. To access any of the terminal servers, a person would have to go through URE's corporate firewalls, authenticate through the Electronic Security Perimeter (ESP) firewall and one of the URE FEP servers, and know the default username and password for the terminal server. Five to fifteen personnel had access to the FEP servers required to gain access to the terminal servers. In addition, SERC determined that URE had a procedure in place to address the removal, disabling or renaming of default accounts, but the procedure was not applied in this case because URE was not aware of the default accounts on the devices at issue.

CIP-004-3 R4.2 (SERC201100776)

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

CIP-004-3 R4 provides in pertinent part:

> R4. Access - The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> ***
>
> 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 R4.2 has a "Lower" VRF and a "Moderate" VSL.

URE submitted a Self-Report to SERC stating that it had discovered a single instance where it failed to revoke access to CCAs within seven calendar days for an employee that transferred to a different department and no longer needed access to CCAs.

The supervisor of an employee with approved unescorted physical access to CCAs sent a request to the URE corporate security department to have the employee's access to CCAs revoked due to a transfer. The supervisor requested that the employee's access rights be removed approximately four days later, the date of the transfer. The corporate security department mistakenly coded the request as "low" priority instead of "high" priority and failed to complete the request on time.

On the day access was supposed to be removed, as part of URE's standard review process, corporate security sent out a routine advisory to all supervisors with a list of their direct reports that had approved access to CCAs and asked that the supervisors confirm that the employee's access rights were still appropriate. Approximately two weeks later, the employee's new supervisor mistakenly responded that the transferred employee should retain all access rights. Since URE's corporate security department had still not processed the original revocation request, the transferred employee retained access to CCAs.

Four days later, URE corporate security sent a quarterly access review list of all CIP-protected areas to the asset approvers for URE. The asset approver responded that the transferred employee should have access to CCAs removed. URE removed the transferred employee's access to CCAs on the same day, which was 18 days after the employee no longer needed access.

SERC determined that URE had a violation of CIP-004-3 R4.2 for failing to revoke, within seven calendar days, approved unescorted physical access to CCAs for an employee who no longer needed such access.

SERC determined the duration of the violation to be from when the employee's access should have been revoked through when URE revoked the employee's access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Prior to and after the violation, the employee was in good standing with URE. URE revoked the employee's access 18 days after the employee no longer needed access. Furthermore, the employee never used or attempted to use his or her access to CCAs after the date of the transfer.

CIP-005-1 R1.4 (SERC2011007429)

The purpose statement of Reliability Standard CIP-005-1 R1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter."

CIP-005-1 R1 provides in pertinent part:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> ***
>
> R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.
>
> ***

CIP-005-1 R1.4 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it had deployed certain network devices inside ESPs that URE did not identify as non-critical Cyber Assets. SERC determined that URE failed to identify approximately three dozen network switches as non-critical Cyber Assets that resided within several ESPs. These network switches provided communication routing for all non-critical Cyber Assets and CCAs that were identified within the ESPs. These network switches were unmanaged devices and only functioned to provide pass-through communications between Cyber Assets. URE did not consider

these network switches to be subject to CIP Standards because they were not assigned Internet Protocol (IP) addresses. The network switches could only be made IP-routable by physically connecting to a management port on each switch and altering the configuration. As such, URE did not identify and protect these devices as either CCAs or non-critical Cyber Assets within the ESP.

SERC determined that URE had a violation of CIP-005-1 R1.4 for failing to identify the network switches as non-critical Cyber Assets within a defined ESP.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The network switches at issue were used as unmanaged switches without IP addresses, making it extremely difficult for an outside attacker to locate, access, or attempt to compromise the switches. The network switches could only be converted to managed switches, or made IP-routable, by physically connecting to a management port on the switches. Furthermore, the network switches were protected inside ESPs and PSPs.

CIP-007-1 R5.2 (SERC2011007639)

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

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management - The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> ***
>
> R5.2. 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).

***

CIP-007-1 R5.2 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it had discovered some CCAs and non-critical Cyber Assets within the ESP with passwords that had not been changed annually. URE had an account management procedure in place that described how administrator, shared, and other generic account privileges should be managed, removed, or renamed. This policy addressed the proper use of passwords and the requirements for password complexity and password changes that should occur annually or more frequently based on risk. Where URE could not adhere to its internal policy due to technical limitations, it submitted TFEs, which were approved.

During its CVA, URE discovered approximately 100 CCAs that had local user or shared application accounts with default passwords that had not been changed annually. These Cyber Assets were not managed pursuant to the URE account management procedure because the URE personnel responsible for the affected Cyber Assets were unaware of the existence of the shared application accounts. As a result, URE failed to implement its internal policy to minimize and manage the scope and acceptable use of the local user or shared application accounts privileges.

SERC determined that URE had a violation of CIP-007-1 R5.2 for failing to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts on CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE changed all the default application account passwords.

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 manage administrator, default and shared accounts properly could have left the CCAs, which were EMS devices, vulnerable to exploitation. However, no more than ten to twenty administrative support personnel with authorized cyber access had knowledge of the credentials associated with the unchanged passwords on the CCAs. In order to use the shared application accounts on these CCAs, an individual would have needed physical access to the Cyber Asset and cyber access or a security token with two-factor authentication with a token code that changed every 60 seconds for remote access. In addition, the CCA application accounts were not used to log on to any other devices within the EMS.

CIP-004-3 R4 (SERC2011007985)

CIP-004-3 R4 provides in pertinent part:

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

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

During a Compliance Audit (Compliance Audit), SERC discovered that URE used a vendor to perform URE's CVA but failed to document its authorization of the vendor for cyber access to CCAs.

URE contracted with an outside vendor to perform URE's CVA addressing CIP-007-3 R8. The four vendor personnel who conducted the CVA were physically escorted while performing the CVA by a single URE employee who was authorized for unescorted physical access. URE allowed the vendor personnel to have cyber access to CCAs, but it did not assign them log-in credentials or capabilities. Instead, URE personnel with authorized cyber access logged-in to the CCAs as necessary and allowed the vendor personnel to conduct the CVA using the URE personnel's credentials, while URE personnel observed the vendors' actions. URE never added the vendor personnel to its list of personnel with authorized cyber access or included the vendor personnel's specific access rights. URE provided the four vendor personnel with cyber access for a period of four days.

SERC determined that URE had a violation of CIP-004-3 R4 for failing to maintain its list of personnel with authorized cyber or authorized unescorted physical access to CCAs with respect to the vendor personnel.

SERC determined the duration of the violation to be from the date the vendor personnel began the CVA and first accessed the CCAs, through when the vendor personnel finished the CVA and no longer accessed the CCAs.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to track and maintain a list of personnel with cyber access to CCAs could have allowed individuals with unauthorized cyber access to CCAs to manipulate or alter those CCAs, either purposefully or by mistake, resulting in disruption or loss of control of the EMS or URE's portion of the BPS. However, URE did not grant log-in credentials to the four vendor personnel conducting the CVA, and URE kept the vendor personnel under observation.

CIP-005-1 R1.1 and R1.5 (SERC2011007986)

CIP-005-1 R1 provides in pertinent part:

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

CIP-005-1 R1.1 and R1.5 each have a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to identify a Cyber Asset which communicated externally and was connected inside the ESP as an access point, in violation of CIP-005-1 R1.1.

Also during the Compliance Audit, SERC discovered that URE failed to afford Cyber Assets used in the access control and monitoring of the ESP the protective measures specified in CIP-005-1 R1.5; specifically, the protections of CIP-005 R2 and R3 and CIP-007 R1, R5.2.3, and R6.5. SERC determined that both audit findings involved the same Standard and Requirement and decided to treat the second audit finding as an expansion of the scope of the violation.

For the CIP-005-1 R1.1 violation, URE utilized an intrusion detection system (IDS) outside the ESP that was connected to a switched port analyzer (SPAN) port on a network switch within the ESP. The network switch used the SPAN port to send network traffic data outside of the ESP to the IDS for analysis and alerting, and thus the SPAN port constituted an access point. Because of its configuration, the network switch was not capable of receiving any data from outside the ESP via the SPAN port. URE did not identify this connection across the ESP boundary as an access point in its ESP documentation. URE believed that because the configuration of the network switch did not allow any external communication to come into the ESP via the SPAN port, and only permitted data to flow out of the ESP, the SPAN port did not constitute an access point.

For the CIP-005-1 R1.5 violation, the SERC audit team found that URE did not afford electronic access control and monitoring (EACM) devices the protective measures specified in CIP-005 R2 and R3, and CIP-007 R1, R5.2.3, and R6.5. URE had several EACM devices that resided outside of an ESP, but were located within a PSP. These devices consisted of logging servers and authentication servers. The EACM devices were connected to a terminal server on URE's corporate network and were not protected within an ESP. The logging servers performed logging and monitoring for both CCAs and devices that were connected to the corporate network. This setup allowed logs from CCAs to pass through the ESP firewall and go to the logging servers for aggregation, review, and alerting as necessary. Access to the logging servers was managed by the authentication servers, which required strong two-factor authentication in order to gain access, and this access was limited to five to ten administrators. All of the administrators had valid PRAs and had received annual cyber security training. In order to gain access to CCAs and EACMs, authentication at the authentication servers was required.

For CIP-005 R2 and R3, URE was able to show organizational processes and technical and procedural mechanisms for control of access to these EACM devices, as well as electronic processes for monitoring and logging access to the EACM devices 24 hours a day, seven days a week. In an effort to protect these EACM devices, however, URE classified them as access points to an ESP, despite being located outside of an ESP. CIP-005 R2 and R3 require organizational and technical controls for electronic access at all electronic access points to an ESP. Because these EACM devices were located on an URE

corporate network and not within an ESP, the electronic access points to the EACM devices in question would be the firewalls protecting the corporate network. URE provided no evidence that the firewalls protecting its corporate network were protected pursuant to CIP-005-1 R2 and R3.

For CIP-007 R1, SERC determined that URE had a test plan established for the EACM devices, but it did not include adequate cyber security testing of security controls after a significant change and had insufficient test results for one EACM. For CIP-007 R5.2.3, SERC determined that URE had no documented policy on how to develop audit trails for the use of shared accounts on the EACM devices. For CIP-007 R6.5, SERC determined that URE failed to review logs of system events related to cyber security and maintain records documenting the review of logs for the authentication servers because those logs were not being sent to the authentication servers.

SERC determined that URE had a violation of CIP-005-1 R1 for failing to identify as an access point a Cyber Asset which communicated externally and was connected inside the ESP. SERC also determined that URE had a violation of CIP-005-1 R1.5 for failing to afford Cyber Assets used in the access control and monitoring of the ESP certain protective measures specified in the Standard.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to identify an access point into the ESP as required by CIP-005-1 R1.1 could have provided information about internal ESP traffic to unauthorized personnel or allowed a potential open access point for unauthorized access to CCAs. However, due to the configuration of the access point, ingress traffic to the ESP was unlikely. A SPAN port, which was configured for egress traffic and not ingress traffic, was connected from the network switch inside the ESP to the IDS outside the ESP. URE's IDS, which monitored for and would alert on any traffic anomalies detected, was protected behind corporate firewalls.

SERC also determined that URE's failure to ensure that EACM devices were afforded the protective measures listed in CIP-005 R1.5 could have allowed malicious individuals to manipulate the EACM devices, allowing unauthorized access to CCAs within the ESP. However, all personnel with electronic access to the EACM devices had current PRAs and had received annual cyber security training. Access to the EACM devices required strong two-factor authentication. All CCAs were within a secured ESP and PSP with IDS monitoring and alerting enabled. In addition, URE afforded the EACM devices some of the protective measures listed in CIP-005-1 R1.5, including antivirus protection, patch management,

strict firewall access control rules on the corporate firewall, some security event logging, and network intrusion detection.

CIP-005-1 R2.2 (SERC2011007987)

CIP-005-1 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ***
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> ***

CIP-005-1 R2.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, URE was unable to provide a current operational need for some of the open ports sampled by SERC. After the Compliance Audit concluded, URE initiated and conducted a comprehensive review of all its existing firewall rules. In addition to the ports and services found during the Compliance Audit, URE's internal review identified several additional ports and services on a few access points to the ESP that were not required for operations and for monitoring Cyber Assets within the ESP. None of the identified ports and services provided remote access into the ESPs.

SERC determined that URE had a violation of CIP-005-1 R2.2 for failing to enable only ports and services required for operations and for monitoring Cyber Assets within the ESP at all access points to the ESP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE disabled the unneeded ports and services on the access points to the ESP.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to disable unnecessary ports and services at

access points to the ESPs could have allowed unauthorized connectivity through the access points, which could have disrupted the normal operations of CCAs. This disruption could have in turn led to a loss of control or visibility over URE's portion of the BPS. However, interactive access to URE CCAs required two-factor authentication. Some URE CCAs could not enforce two-factor authentication; these CCAs could only be accessed through other CCAs that required two-factor authentication. URE used a security configuration management system that tracked ports and services on all CCAs and would send real-time alerts to URE personnel for any suspicious port or service detected. URE also used a centralized log aggregation server to provide immediate alerts for any suspicious activity logged from any CCA. All of URE's CCAs capable of running antivirus software were protected by antivirus software. Furthermore, URE's ESP firewalls were protected behind multiple firewalls within the corporate network.

CIP-005-1 R4.2 (SERC2011007988)

CIP-005-1 R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> ***

CIP-005-1 R4.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to include a review of ports and services that are allowed access through the access points in its CVA of the electronic access points to the ESP.

URE had a CVA process for CIP-005-1 R4 and URE conducted the required CVAs. The CVA process required a review of ports and services at the access points to the ESP, but the process did not require a review of the firewall rules for ports and services allowed through the access points. URE believed that CIP-005-1 R4.2 only required it to review the ports and services at the electronic access point and not the ports and services (firewall rules) allowing communications into and out of the ESP. As a result, URE only reviewed the ports and services that were enabled on the physical Ethernet ports on the firewalls. URE believed that a review of ports and services allowed through the firewall was not

required under CIP-005-1 R4. As a result, during its annual CVAs, URE did not review the firewall rules and associated electronic ports and services that were enabled to allow information to pass through the physical access points on the firewalls.

URE initiated and documented a review of all firewall rules. During this review, URE discovered several open ports that needed to be disabled.

SERC determined that URE had a violation of CIP-005-1 R4.2 for failing to include, in its annual CVA, a review of ports and services allowing communications into and out of the ESP to verify that only ports and services required for operations were enabled.

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

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to review the firewall rules for unnecessary ports and services through access points to the ESP rendered those ports and services vulnerable for an extended period of time to unauthorized connectivity, which could have disrupted the normal operations of CCAs within the ESP. Such a disruption to CCAs could have in turn led to a loss of control or visibility over URE's portion of the BPS. However, interactive access to most URE CCAs required two-factor authentication. Access to those CCAs that could not enforce two-factor authentication could only be made through CCAs that required two-factor authentication. In addition, URE had a change management process that required a formal review and approval of all proposed firewall rules before implementation that minimized ports from being enabled without an identified need. After its firewall rule review, URE found several ports that needed to be disabled.

Moreover, URE used a security configuration management system that tracked ports and services on certain CCAs and would send real-time alerts to URE personnel for any suspicious port or service detected. URE also used a centralized log aggregation server to provide immediate alerts for any suspicious activity logged from any CCA. As technically feasible, URE's CCAs were protected by antivirus software. In addition, URE deployed IDS to monitor for malicious or anomalous traffic, including the ingress point of the access points in question. Lastly, URE's ESP firewalls were protected behind multiple firewalls within the corporate network.

CIP-006-1 R1.7 and R1.8 (SERC2011007989)

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

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> ***
>
> R1.7. 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.
>
> ***

CIP-006-1 R1.7 has a "Lower" VRF and a "Severe" VSL. CIP-006-1 R1.8 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to define a PSP properly. SERC also discovered that URE failed to afford the Cyber Assets used in the access control and monitoring of the PSP, or Physical Access Control System (PACS) devices, all of the protective measures specified in CIP-006-1 R1.8. SERC determined that both audit findings involved the same Standard and Requirement and decided to treat the second audit finding as an expansion of the scope of the violation.

SERC determined that URE's physical security plan included provisions addressing Requirements R1.1 through R1.8 and it specified actions necessary for the creation of a secured physical perimeter. However, SERC discovered that URE's documentation incorrectly marked the PSP boundary in its

physical security plan, showing the PSP as extending further than it actually did. URE updated the boundary drawing immediately upon discovery, and SERC auditors confirmed the correct PSP boundary was documented while on-site. SERC considered this violation of CIP-006-1 R1.7 to be a documentation issue, and not an operational or functional failure.

For the CIP-006-1 R1.8 violation, SERC determined that URE did not afford its PACS devices all the protective measures listed in CIP-006-1 R1.8. Specifically, SERC determined that the identified PACS devices were not afforded the protections of CIP-005 R2 and R3, CIP-007 R4.2, CIP-007 R5.2.1 prior to deployment, and CIP-007 R5.2.

URE had identified a few PACS servers that provided the primary access control and authorization to PSPs as Cyber Assets. These servers were used to grant access to PSPs, store logs of access, and store lists of authorized personnel with unescorted access rights. URE deployed the PACS servers on its corporate network and maintained them within established PSPs, but it failed to provide them with the protective measures listed in CIP-006 R1.8. URE limited electronic access to the PACS servers to 5 to 10 system administrators, all of whom had current PRAs and annual cyber security training. However, the PACS servers were also electronically accessible by a number of general users who could access card access workstations that were attached to the PACS servers. As a result, the general users had the ability to create new access badges, alter physical access rights on existing access badges, or manipulate secured PSP doors. URE is unaware of any users, other than 5 to 10 administrative support personnel with authorized cyber access, who knew they had such access.

URE failed to provide its PACS servers the protective measures specified in CIP-005 R2 and R3. URE was unable to show organizational processes and technical and procedural mechanisms for the control of electronic access to the corporate network in which the PACS servers resided, and could not demonstrate electronic processes for monitoring and logging access to the PACS servers at all times.

URE failed to provide its PACS servers the protective measures specified in CIP-007 R4.2. URE depended on the vendor to provide testing and implementation of antivirus and malware prevention signatures on its PACS servers. Since these servers were on the corporate network, all the updated signatures were pushed automatically during scheduled updates. URE was unable to provide evidence that all the updated signatures were tested and installed as required.

URE failed to provide its PACS servers the protective measures specified in CIP-007 R5.2.1. URE failed to change shared default accounts on the PACS servers. These accounts were needed to provide a way to acknowledge alarms received that could not be managed through normal actions (known as “orphaned alarms”). The account passwords in question were hard-coded and could not be changed

by URE. This was a known problem, and URE documented an exception to its policy, had the manual from the vendor outlining the issue, and maintained correspondence with the vendor seeking alternative solutions to this problem.

URE also failed to provide its PACS servers the protective measures specified in CIP-007-1 R5.2. URE failed to change some account passwords annually on a few PACS devices. URE initially submitted a Self-Report detailing this violation. Because the SERC audit team found additional violations of CIP-006-1 R1.8 involving PACS devices, SERC decided to address the portion of the violation from the Self-Report that dealt with PACS devices with the other CIP-006-1 R1.8 violations found during the audit. During its CVA, URE discovered a few PACS devices that had local user or shared application accounts with default passwords that had not been changed annually. These Cyber Assets were not managed pursuant to the URE account management procedure because the subject matter experts responsible for the affected Cyber Assets were unaware of the existence of the shared application accounts. As a result, URE failed to implement its internal policy to minimize and manage the scope and acceptable use of the local user or shared application accounts privileges. No more than 5 to 10 administrative support personnel with authorized cyber access had knowledge of the credentials associated with the unchanged passwords on the PACS devices.

URE submitted another Self-Report to SERC stating that it failed to afford some of its PACS devices any of the protective measures specified in CIP-006-1 R1.8. SERC determined that this Self-Report was directly related to the audit findings, which involved the same Standard and Requirement, and decided to treat this Self-Report as an expansion of the scope of the audit findings.

SERC determined that URE failed to identify all of its PACS devices. Originally, URE identified a few PACS servers as Cyber Assets. URE failed to consider and identify as Cyber Assets card access workstations, which could be used to update the physical access rights on existing access badges and to create new access badges. URE also failed to consider and identify as Cyber Assets card access system panels, which provided local cached memory to the badge readers and provided temporary storage of access logs. The card access workstations and card access system panels were not located within an ESP or PSP. In addition, URE had a number of general users with access to the card access workstations that had the capability to alter the physical access rights on existing access badges and create new access badges. URE is unaware of any users, other than 5 to 10 administrative support personnel with authorized cyber access, who knew they had these abilities. Because it failed to identify them as Cyber Assets, URE did not provide the card access workstations and the card access system panels any of the protective measures specified in CIP-006-1 R1.8.

SERC determined that URE had a violation of CIP-006-1 R1.7 for failing to mark the PSP boundary properly in its documentation. SERC determined that URE had a violation of CIP-006-1 R1.8 for failing to afford the PACS devices and servers all of the protective measures specified in the Standard.

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, URE's failure to document the boundary of a PSP correctly, as required by CIP-006-1 R1.7, could have led to inadequate protection or omission of access points to the PSP. However, SERC considered this violation to be strictly a documentation error, and all CCAs and non-critical Cyber Assets within the ESP were secured within an established PSP.

URE's failure to provide its PACS servers with all of the protective measures listed in CIP-006-1 R1.8 and its failure to identify devices as PACS devices could have left those PACS devices vulnerable to electronic or physical manipulation, which in turn could have allowed unauthorized individuals to gain physical access to CCAs protected within PSPs. In addition, by allowing users the ability to log on to the PACS servers and card access workstations, which could be used to change physical access permissions on existing access badges and create new access badges, URE increased the risk that unauthorized individuals could gain physical access to CCAs protected within PSPs. However, the following factors mitigated the risk. The PACS servers were secured with a PSP that utilized alarm monitoring. URE knew of the existence of the PACS devices that it failed to identify as Cyber Assets, and it protected the PACS devices and PACS servers behind corporate firewalls. In order to change the physical access rights of an individual, the general users and 5 to 10 administrative users of the card access workstations needed a valid username and password for the workstation and a valid username and password for the card access application. Furthermore, URE is unaware of any users, other than 5 to 10 administrative support personnel with authorized cyber access, who knew they had the ability to create new access badges or alter physical access rights on existing access badges.

CIP-007-1 R2.2 (SERC2011007990)

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

CIP-007-1 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 R2.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to disable ports and services not required for normal and emergency operations. Following its CVA, URE identified nine ports on several CCAs that were not disabled and were potentially not required for normal and emergency operations. This violation affected less than five percent of URE's CCAs. URE was in the process of investigating the need for the nine identified ports at the time the Compliance Audit occurred.

URE attested that it needed five of the ports to remain enabled and that it would disable the four remaining ports in accordance with the CVA action plan. URE used the four remaining ports for remote support. These ports allowed URE access to and the ability to transfer data to and from the CCAs within the same ESP. URE determined these ports were not required because it could perform the support function using local serial access. URE restricted access to these four identified ports to no more than ten screened and trained administrative users.

SERC determined that URE had a violation of CIP-007-1 R2.2 for failing to disable ports and services not required for normal and emergency operations.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE discovered this violation during its annual CIP-007 CVA and was actively working to resolve it pursuant to its CVA action plan. The CCAs with the unneeded ports were for firmware-only devices, and no third-party software could be installed. Furthermore, URE restricted and limited access to the four ports at issue to no more than 10 authorized personnel whom URE had screened and trained for authorized cyber access.

CIP-007-1 R8.3 (SERC2011007992)

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

CIP-007-1 R8 provides in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R8.3. A review of controls for default accounts . . .
>
> ***

CIP-007-1 R8.3 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC discovered that URE failed to review the controls for default accounts for applications running on Cyber Assets within the ESP.

SERC determined that URE reviewed operating system default passwords as part of the CVA process for its EMS. URE used dedicated workstations for the EMS and required the use of operating system passwords with a token and pin number (strong, two-factor authentication) to log on to the EMS. Application or database passwords could not be used to authenticate to the EMS and were only used to start the application on the EMS workstation after logging-in using the strong, two-factor authentication. URE believed that it was required to review accounts which provided initial access to Cyber Assets. However, URE incorrectly believed that it was not necessary to review the internal,

network-inaccessible accounts used by personnel to start the applications that were only accessible once cyber access had been granted via the strong, two-factor authentication.

SERC found that URE's CVA process document directed users to establish and document the methods and tools to be used in the execution of the annual CVA and required that the established plan be reviewed to ensure it met URE expectations and received prior approval before being executed. The document also required that the CVA methodology be conducted on a representative group of test Cyber Assets prior to being performed in the production environment to demonstrate there were no potential operational impacts. However, SERC determined that URE's CVA document simply restated the CIP requirements for CIP-007-1 R8 and CIP-005-1 R4 in lieu of providing sufficient details on how to perform the CVA. Significantly, SERC found that the CVA document did not direct URE personnel to review the controls for default accounts.

SERC found that URE's second CVA document provided more detail than the first CVA document about what was expected to occur during the execution of the annual CVA, including statements detailing what would be done to ensure compliance with each requirement. The second CVA process required, under CIP-008-1 R8.3, that URE examine configuration files to ensure there were no local accounts with the factory default password enabled, examine lists of operating systems on Cyber Assets, and examine application servers for each Cyber Asset within the ESP to determine the status of any default or generic accounts. This was done to ensure the URE policy for account management was followed, and that no default or generic accounts were in use.

SERC determined that URE had a violation of CIP-007-1 R8.3 for failing to review the controls for default accounts for applications running on Cyber Assets within the ESP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE revised its CVA process to include a review of application accounts and passwords.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE used EMS-dedicated workstations that required strong, two-factor authentication in order to log-in and have access. Application or database passwords could not be used to gain access to the URE EMS. Furthermore, the workstations were located in a control center that was manned at all times.

CIP-007-1 R1 (SERC2011007993)

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

CIP-007-1 R1 provides in pertinent part:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> ***

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

During the Compliance Audit, SERC discovered that URE failed to have a formal test procedure for significant changes to Cyber Assets. In addition, the test procedures provided by URE did not cover all security controls as required by CIP-007-1.

URE's testing procedures required that URE complete a risk worksheet for any proposed change to any Cyber Asset within the ESP. This worksheet established a risk value in order to determine the significance of the change. The cyber security test plan required that all proposed changes classified as significant be reviewed and approved by an URE change board. If the URE change board approved the change, URE would conduct all necessary testing and would create a change ticket to document the testing and results. URE retained evidence of cyber security controls testing in the ticketing system and showed the historic comparison of the configuration files and ports and services before and after the significant change.

However, SERC determined that the testing procedures did not specifically address what testing steps would occur and in what manner testing would occur. Instead of providing a standard set of documented test steps based on the Cyber Asset, the URE test procedure required a before and after comparison of the configuration files and ports and services. The test procedure did not require a review to confirm that antivirus programs were still running, that default accounts were not introduced, that ports or services were not newly enabled, and so on. SERC determined that these test

procedures were inadequate to ensure that significant changes to existing Cyber Assets did not adversely affect existing cyber security controls.

In the history of one terminal server CCA, one significant change was performed. URE performed an internal review of the device and found no additional changes occurred that rose to the level of a significant change to an existing Cyber Asset.

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

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE updated its testing procedure to require full testing of cyber security controls after significant changes to existing Cyber Assets.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had one CCA that was subject to its testing procedure, and one significant change was performed in the history of the device. In addition, URE conducted some testing which could have revealed some changes to existing cyber security controls. Specifically, URE compared the before and after configurations of the configuration files and ports and services.

CIP-006-3c R2.2 (SERC2012010331)

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

CIP-006-3c R2 provides:

> R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and/or log access to the Physical Security Perimeter(s), exclusive of hardware at the Physical Security Perimeter access point such as electronic lock control mechanisms and badge readers, shall:
>
> R2.1. Be protected from unauthorized physical access.
>
> R2.2. Be afforded the protective measures specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirements R4 and R5; Standard CIP-007-3; Standard CIP-008-3; and Standard CIP-009-3.

CIP-006-3c R2.2 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report stating that it failed to afford PACS devices the protective measures specified in CIP-006-3c R2.2. Specifically, URE failed to issue alerts related to potential Cyber Security Incidents for PACS devices as specified by CIP-007-3 R6.2.

URE had a physical security plan which specified that all Cyber Assets that authorize and/or log access to URE's PSPs should be protected from unauthorized physical access. URE also maintained a security status monitoring procedure that detailed how to handle alerts for cyber security events on CCAs, non-critical Cyber Assets within the ESP, and access points to any PSP and ESP, using an automated alert tool. The procedure also required URE analysts to manually review the logs for any Cyber Security Incidents within seven days of a failure of the automated alerting tool.

URE realized that it was not receiving any email alert notifications related to log-in activity from Cyber Assets for its PACS. Upon further review, URE discovered that this issue started approximately four months earlier, and was isolated to the PACS Cyber Assets. No other Cyber Assets were affected because they were located in a separate ESP. URE determined that a memory issue in the automated tool used to review and alert for potential Cyber Security Incidents caused the alerts for the PACS servers to be dropped. The security logs from the PACS devices were being received by the automated alert tool as required, and the security logs were being retained, but the alerts out of the automated tool about security conditions potentially affecting the PACS Cyber Assets failed to occur.

URE manually reviewed and verified all of the security logs from the PACS devices after discovery, and found no actual Cyber Security Incidents that required action.

SERC determined that URE had a violation of CIP-006-3c R2.2 for failing to afford PACS devices the protective measures specified in the Standard--specifically, automated or manual alerts for potential Cyber Security Incidents (CIP-007-3 R6.2).

SERC determined the duration of the violation to be from when URE's automated alerting tool stopped working for its PACS devices through when URE reviewed the logs generated by the tool for PACS devices.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE reviewed all user accounts on the PACS servers each month and found no suspect accounts. In order to make any modifications to access rights, an individual would have needed application accounts and a password for the PACS servers. In addition, after discovering this issue, URE

manually ran all the PACS logs from the duration of the alerting failure through its alerts system and discovered no actual Cyber Security Incidents that required action.

CIP-004-3 R2.1 (SERC2012011169)

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

CIP-004-3 R2 provides in pertinent part:

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

***

CIP-004-3 R2.1 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it discovered a single individual who was granted access to a CCA without completing the cyber security training within the last year. Following a review, SERC determined that URE failed to provide cyber security training to the individual before granting access to CCAs, a violation of CIP-004-3 R2.1.

A URE employee requested electronic access to a CCA through an internal request tool. The employee had previously been authorized to access CCAs, but because the employee's need for access had changed, URE revoked the employee's access to CCAs prior to the request. Approximately ten days later, URE approved and granted authorized electronic access to the employee in error though the internal request tool. Approximately four days later, URE became aware of this error though a bi-weekly check process it used to ensure that personnel access rights aligned with need. Two days after discovery, URE revoked the employee's access rights pending completion of the cyber security training.

SERC determined that URE had procedures in place requiring URE personnel responsible for authorizing access to CCAs to verify the completion of cyber security training and a current PRA before granting access. However, due to human error, the employee's lack of current cyber security training was overlooked in this case, and the individual was granted access to CCAs. The employee did not use or attempt to use his or her access rights during the period he or she had authorized cyber access.

SERC determined that URE had a violation of CIP-004-3 R2.1 for failing to have a program that ensured that all personnel having authorized cyber or authorized unescorted physical access to CCAs were trained prior to being granted such access.

SERC determined the duration of the violation to be from when URE granted the employee authorized cyber access without ensuring that the cyber security training had been completed, through when URE revoked the employee's access.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The employee in question had a valid PRA and had previously been authorized to have cyber access to CCAs. Furthermore, the employee was in good standing with URE prior to and after this incident.

CIP-006-3c R1.6 (SERC2013012004)

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

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

> R1. Physical Security Plan — The Responsible Entity shall document, implement, and maintain a physical security plan, approved by the senior manager or delegate(s) that shall address, at a minimum, the following:
>
> ***
>
> R1.6. A visitor control program for visitors (personnel without authorized unescorted access to a Physical Security Perimeter), containing at a minimum the following:
>
> R1.6.1. Logs (manual or automated) to document the entry and exit of visitors, including the date and time, to and from Physical Security Perimeters.

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

***

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

URE submitted a Self-Report to SERC stating that it had discovered multiple failures by authorized personnel to follow the URE visitor control program while escorting personnel within PSPs.

URE's visitor control program required that authorized personnel maintain visual contact with the escorted personnel at all times while within the PSP and not exceed the maximum number of visitors allowed to be escorted by any single authorized personnel at any one time. URE discovered that its personnel had not followed the visitor control program in three instances.

URE discovered that a contract employee was left unescorted in a PSP for approximately five minutes. Security personnel made this discovery while investigating video footage for the cause of an unrelated and non-PSP door alarm received at the security console.

On a second date, URE discovered that an authorized escort failed to follow the visitor control program while escorting contract cleaning crews within a PSP. URE determined that there had been four instances where this individual escorted more than the allowed number of cleaning personnel, despite the visitor control program's limit of escorting no more than a specified number of unauthorized personnel by a single escort. URE also discovered that this authorized escort had left cleaning personnel unescorted for between one to seven minutes on three separate occasions.

URE discovered a third failure while reviewing its second discovery. This third failure involved a separate cleaning crew contracted to clean a PSP approximately one month prior. Over the span of one night, two members of a cleaning crew were authorized to serve as escorts for the remainder of the cleaning crew. URE discovered that, on five separate occasions during the night, one of the authorized escorts left the PSP, leaving one escort with more than the allowed number of escorted personnel. URE also discovered that on three separate occasions during the night, the unauthorized personnel were left without any escort for between one to eight minutes.

SERC determined that URE had a violation of CIP-006-3c R1.6 for failing to provide a continuous escort to visitors while within the PSP and for failing to maintain no more than the allowed ratio of visitors to authorized escorts, as required by the URE visitor control program.

SERC determined the duration of the violation to be from the date that URE first failed to escort visitors performing cleaning duties in a proper manner through the last date a visitor was not escorted properly.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability BPS. URE failed to provide continuous escort for between one to eight minutes in each instance. All the affected sites have closed circuit cameras which record video at the entrances and exits for the PSPs. All Cyber Assets within the affected PSPs required a user name and password, at a minimum, to log-in and would alert security for immediate investigation in the event of multiple failed log-in attempts. In the second and third instances discovered by URE, all of the cleaning crew members underwent background checks through their primary employer prior to being hired. Furthermore, the affected sites were staffed and had on-site security personnel at all times.

CIP-007-1 R3 (SERC2013012236)

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

CIP-007-1 R3 provides:

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

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

URE submitted a Self-Report to SERC stating that it failed to document the assessment of security patches and security upgrades for non-critical third-party software on CCAs, EACM devices, and PACS devices (collectively, non-critical third party software) for applicability within 30 calendar days of availability of the patches or upgrades.

URE tracked security patches for operating systems and its primary applications on its EMS, its PACS, and its EACM system. However, URE failed to address the patching of all non-critical third-party software running on Cyber Assets within the ESP in its security patch management program. URE conducted a complete review of all software running on Cyber Assets within its ESPs. URE determined that nearly half of its software applications were not tracked for security patches.

SERC determined that URE had a violation of CIP-007-1 R3 for failing to address the tracking, evaluating, testing, and installing of applicable cyber security software patches for non-critical third-party software on CCAs, EACM devices, and PACS devices in the ESP.

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

SERC determined that this violation posed a serious or substantial risk to the reliability of the BPS. URE's failure to identify and assess applicable security patches for non-critical third-party software within 30 days and apply them in a timely manner could have allowed security vulnerabilities on Cyber Assets to remain unaddressed for extended periods of time, presenting a potential path for unauthorized electronic access and compromise of the BPS. However, SERC also considered the following factors. URE tracked security patches for operating systems and its primary applications on its EMS, its PACS, and its EACM system. URE utilized an IDS to monitor for malicious and anomalous activity and alert for any suspicious access attempts. Logs from Cyber Assets were sent to a centralized logging system and reviewed for any suspicious activity, and any detected suspicious activity would result in a real-time alert to individuals responsible for follow-up investigation. All Cyber Assets, as technically feasible, had antivirus and malware software installed. Where not technically feasible, URE has put compensating measures in place. In addition, URE CCAs were isolated behind access points and were not internet-accessible.

Regional Entity's Basis for Penalty

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported several of the violations;[4]
3. URE was cooperative throughout the compliance enforcement process;
4. URE had an internal compliance program (ICP) at the time of the violations which SERC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. 17 of the 19 violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. 2 of the 19 violations posed a serious or substantial risk to the reliability of the BPS, as discussed above;
8. URE has unified and standardized most of its CIP procedures across departments to ensure compliance. In addition, URE has restructured its physical security organization and personnel to enforce compliance with CIP Standards, and it has implemented controls and crosschecks to ensure future compliance. SERC considered these actions to be a mitigating factor;
9. URE has expended substantial resources to improve compliance and to implement mitigation action to correct violations. Specifically, URE is implementing a new best practices card access system and purchasing additional firewalls, providing cyber security training to all URE personnel, and expanding its compliance staff. SERC considered these expenditures to be a mitigating factor;
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of one hundred and twenty thousand dollars ($120,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

[4] URE self-reported the violations of CIP-004-1 R4 (SERC200900284), CIP-007-1 R5 (SERC201000586), CIP-004-3 R4 (SERC201100776), CIP-005-1 R1 (SERC2011007429), CIP-007-1 R5 (SERC2011007639), CIP-006-3c R2 (SERC2012010331), CIP-004-3 R2 (SERC2012011169), CIP-006-3c R1 (SERC2013012004), and CIP-007-1 R3 (SERC2013012236). SERC did not award self-report credit for the Self-Reports associated with violations CIP-004-1 R2 (SERC201000551), CIP-004-1 R4 (SERC201000552), or CIP-006-1 R1 (SERC2011007989).

Status of Mitigation Plans[5]

CIP-004-1 R4 (SERC200900284)

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

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

URE's Mitigation Plans required URE to:

1. as an interim measure, manually generate e-mail notifications to URE security informing security of any lateral transfer of a consultant so that security can revoke access and update the access list in a timely manner;
2. as a permanent measure, make necessary changes in the software utilized by URE so that it would trigger a notification to security for a lateral transfer of a consultant;
3. retrain its employees and implement a procedure in which security department employees cross-check the work from prior days on access matters to ensure that access profiles are properly modified;
4. develop and implement a process for checking and approving every step for granting access, including defining the steps to follow-up with supervisors upon receiving an employee's transfer modification, and train personnel on the new process;
5. develop and issue an advisory on at least a quarterly basis for supervisors to review access lists of their employees and consultants;
6. revise a computerized process to include identification of time-sensitive workflows and train security personnel on selecting appropriate due dates when creating assignments for time-sensitive workflow notifications;
7. produce an automated report of all personnel changes from the previous day, and require security personnel to review the report at least every seven calendar days and verify that notifications of the corresponding access changes were received;

[5] *See* 18 C.F.R § 39.7(d)(7).

8. produce an automated report of all card access system changes from the previous day, require security personnel to review the report every seven calendar days to ensure that any changes are accurate and appropriate, and train security personnel on this new process;
9. produce an automated report of all active card access system badge holders with access to CCAs that have non-active accounts in its access control system, and require security personnel to review this report every seven calendar days;
10. create a computer based training to clarify the importance of responding to the supervisor advisory in a timely manner, training which will be reviewed, revised, and administered at least annually; and
11. train appropriate personnel on changed procedures and processes.

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

1. an e-mail with daily manual notifications and a copy of a spreadsheet attachment; email samples of daily manual notifications, which are described as a temporary measure until it can be automated; a sample of daily badge modification verification log sheets showing the notification date if there was a manual notification, and what actions were taken by the security department; a copy of the revised corporate security badge procedures; copies of training records for employees that were retrained; and example logs of work verification showing who verified the removal or change of access from the previous day's work and the date verified;
2. an e-mail stating that coding has been tested and put in to production for the updates to implement a consultant transfer workflow; an email of an automatic workflow triggered by a department change of an employee and needing immediate response by the department responsible for access badges; samples of automatic workflows generated on four separate dates; and sample log sheets which include the notification date and indication of the type of notification (manual or automatic) and what actions were taken by security, demonstrating that the automatic notification was working properly;
3. a revised URE corporate security badge procedure which now includes a cross-check of all access changes from the prior day; training records for employees that demonstrate that the security department completed retraining its badging personnel on the new procedures; and an example log of work verification showing who verified the removal or change of access from the previous day’s work and the date verified;

4. a copy of the URE corporate security access request verification form that describes the revised process; a copy of the training records for employees showing that the security department completed retraining its badging personnel on the new process; and screen shots of the web site showing the access request verification forms that have been completed for a few individuals;
5. an email advisory addressed to supervisors emphasizing the importance of timely completion of paper work for any job status changes (transfer and termination) and to collect badges for terminations, and screen shots of the compliance acknowledgements email box showing acknowledged receipt of the above emails;
6. a screenshot of revised URE corporate security process and an email showing that corporate security department personnel were instructed to select the appropriate due date for time-sensitive workflows;
7. an email from information technology stating that the new automated report is in production, and a copy of a transfer and status change report;
8. a copy of the revised URE corporate security badge procedures incorporating the new process and a copy of training records for security personnel for training on the new process; a change management request showing that the new automated report was put into production; an email stating that the modifications to the card management system report had been implemented; a copy of the URE corporate security badge procedure reflecting the change in process; a training record for security personnel training addressing the updated instructions to use the master access change report; a signed verification view showing review of card access system changes as evidence the system was in place and working and in use; and training records for security personnel for training on the new corporate security badge procedures;
9. an email showing that the results of the automated report that indicates whether any badge holders that have unescorted access to NERC assets that also have non-active accounts in URE's human resource software. No such badge holders were found; and
10. a copy of the training slides emphasizing the importance of responding to the supervisor advisory in a timely manner and the training record for supervisors.

After reviewing URE's submitted evidence, SERC verified that URE's Mitigation Plans were completed.

CIP-004-1 R2.1 (SERC201000551)

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

URE's Mitigation Plan required URE to:

1. revise its cyber security training procedure to comply with Version 2 of CIP-004 by requiring that the cyber security training be completed prior to authorization of unescorted physical access to CCAs;
2. train personnel who had been granted physical access to CCAs and still required physical access to CCAs; and
3. revoke physical access to CCAs for personnel who did not require physical access to CCAs.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted an updated cyber security training program that does not allow URE to grant individuals access to CCAs until those individuals have completed the necessary cyber security training.

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

CIP-004-1 R4.1 (SERC201000552)

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

URE's Mitigation Plan required URE to:

1. create a flowchart to develop an authorized cyber access database. This database checks the status changes of personnel with authorized cyber access to CCAs at least every seven days to identify personnel that have been transferred or terminated in the personnel administration system. The database includes the embedded AD groups for each authorized individual;
2. create an authorized cyber access test database using the new flowchart;
3. place the authorized cyber access test database into production after satisfactory test results; and
4. revise the CIP-004 R4 procedure to implement the process for the new cyber access database and complete training applicable personnel.

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

1. a flowchart used to develop a database to check for status changes of personnel with authorized cyber access to CCAs;
2. an email from URE to SERC advising that the database had been created;
3. a screenshot of test records showing a directory listing of files;
4. an internal URE email advising URE personnel that the database had been placed into production;
5. an updated personnel and training procedure addressing electronic access to CCAs that describes the database its associated query capabilities and the need to validate personnel access;
6. an email confirming the Mitigation Plan and the list of supervisors that would receive the weekly personnel access check via email;
7. an email confirming the addition of supervisors to the list of supervisors receiving the weekly personnel access check via email;
8. an email confirming the addition of an additional supervisor to the list of supervisors receiving the weekly personnel access check via email; and
9. an email confirming no change in the status of URE personnel with access to CCAs.

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

CIP-007-1 R5.2.1 (SERC201000586)

URE's Mitigation Plan to address its violation of CIP-007-1 R5.2.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change the default account password on the terminal servers; and
2. create a procedure that includes a sign-off sheet for vendors to verify that, during the installation process for new hardware or software, they renamed, disabled, removed, or changed passwords for default accounts prior to putting the new hardware or software into production.

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

1. a screen shot of showing the annual update of passwords task and a screen shot showing the completion of the password change; and
2. an updated default account procedure that details the process, responsibilities, and signoff for vendor default accounts.

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

CIP-004-3 R4.2 (SERC201100776)

URE's Mitigation Plan to address its violation of CIP-004-3 R4.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create an additional procedure to specifically outline the process for setting work assignment priority; and
2. train the appropriate security personnel on this procedure.

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

1. a corporate security badging assignment creation procedure with detailed explanation for each step in the procedure.
2. training records showing that the individuals who took the training have read and understand the corporate security badging assignment creation procedure.

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

CIP-005-1 R1.4 (SERC2011007429)

URE's Mitigation Plan to address its violation of CIP-005-1 R1.4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify all network switches inside the ESPs and create a list of these devices;

2. test managed switches inside the EMS environment to determine how they could meet the CIP requirements;
3. draft new CIP procedures or revisions to current CIP procedures to address processes to meet CIP requirements for the network switches;
4. based on the results of testing the managed switches inside the EMS environment, install any new network infrastructure changes that may be needed to support managed switches;
5. finalize the CIP procedures for network switches;
6. update the CCA list by adding network switches; and
7. file TFEs with SERC for network switches for the requirements which could not be met due to technical infeasibility.

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

1. a list documenting the location and number of network switches by type;
2. an email thread establishing network switch testing and identifying a test site;
3. a list of draft procedures URE needed to update in order to mitigate the violation involving network switches. These procedures included URE's CCA list and its CIP recovery plan;
4. an attestation confirming that the switch testing was completed and no infrastructure changes were needed to support managed network switches;
5. updated procedure documents that addressed network switches, including URE's CCA list and its CIP recovery plan;
6. an updated CCA list that included network switches identified as CCAs; and
7. a TFE request sent to SERC that identifies devices that cannot meet the antivirus requirements of CIP 007-1 R4.

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

CIP-007-1 R5.2 (SERC2011007639)

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

URE's Mitigation Plan required URE to:

1. change all CCA local and shared non-application account passwords that were identified in the CVA as not having their passwords changed annually;
2. install software that will identify all non-application accounts on CCA devices to help track accounts that need their passwords changed annually;
3. review and change EMS application account passwords; and
4. revise its account management procedure to include the changing of application passwords as part of the annual password change process.

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

1. a screen shot of URE's ticketing system showing a ticket that was used to identify the devices with passwords that needed to be changed, and showing that the passwords were changed;
2. a screen shot of URE's ticketing system showing a ticket that was used to track the installation and configuration of a password manager that is used to change non-application passwords as needed;
3. a screen shot of URE's ticketing system showing the initiation and changing of passwords for application accounts, as well as the closure of the ticket; and
4. an updated account management procedure in which the password management section has added language requiring the automatic (when possible) or manual changing of passwords, and also specifies the minimum password configuration.

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

CIP-004-3 R4 (SERC2011007985)

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

URE's Mitigation Plan required URE to:

1. revise its cyber security training program to include information stating that any personnel that logs on or electronically uses a CCA needs to be authorized for cyber access even if physically escorted by authorized personnel to do work on a CCA;

2. retrain all personnel with authorized unescorted physical access or authorized cyber access to CCAs using the revised NERC training; and

3. revise its CIP-004 procedures to state that any personnel that will log on or electronically use a CCA needs to be authorized for cyber access even if physically escorted by authorized personnel to do work on a CCA.

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

1. a cyber security training document that discusses unescorted access, escorted access, escort responsibilities, and other aspects of access and escort responsibilities. At the end of the training document, there is a test and a signed acknowledgement of completing and understanding the policies;
2. an email thread confirming the training has been completed and the storage location of the training evidence; and
3. an updated CIP-004 personnel and training procedure that clearly denotes that an individual without authorized cyber access may not electronically log on or use a CCA.

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

CIP-005-1 R1.1 and R1.5 (SERC2011007986)

URE's Mitigation Plan to address its violation of CIP-005-1 R1.1 and R1.5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revise the procedure for testing security controls on EACMs after a significant change;
2. revise the procedure for documenting audit trails on EACMs;
3. revise the procedure for documenting the monitoring and review of logs on EACMs;
4. revise a procedure to include the annual review of access privileges for EACMs;
5. evaluate different options to put EACMs behind an electronic access point to meet the protective measures in CIP-005 R2 and R3;

6. draft new CIP procedures or revise the current CIP procedures to address the access points for EACMs;
7. install new infrastructure to be the access point for the identified Cyber Asset that only communicates externally and is connected inside the ESP;
8. use the selected option for putting EACMs behind an electronic access point, install the new EACM assets behind an electronic access point, and initiate testing;
9. complete testing of the new EACMs and put them into production;
10. finalize the new or revised CIP procedures to address the electronic access points for EACMs; and
11. file TFEs with SERC for the requirements which cannot be met due to technical infeasibility for the electronic access points for EACMs.

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

1. an updated security controls testing procedure that requires testing security controls on EACMs after a significant change;
2. an updated procedure for documenting audit trails on EACMs;
3. an updated procedure for documenting the monitoring and review of logs on EACMs and an email confirming that EACM logs were being reviewed pursuant to the revised procedure;
4. an updated procedure for documenting the annual review of access privileges for EACMs and a review showing that URE followed the updated procedure and conducted an annual account review of access privileges for EACMs;
5. an attestation certifying that the evaluation of different options to put EACMs behind an electronic access point to meet the protective measures in CIP-005 R2 and R3 was completed and indicates the decision that was ultimately made as to how to put the EACMs behind an electronic access point;
6. a screen shot of a web site showing two new CIP procedures and several new TFEs to address the access points for EACMs.
7. an email stating that new infrastructure had been installed to be the access point for the identified cyber asset that only communicates externally and is connected inside the ESP;
8. an email stating that the new EACMs were behind a firewall and testing had started;

9. an email stating that the new EACMs were in production after testing was completed;
10. two updated CIP procedures to address the electronic access points for EACMs; and
11. TFEs that were filed with SERC for the requirements which cannot be met due to technical infeasibility for the electronic access points for EACMs.

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

CIP-005-1 R2.2 (SERC2011007987)

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

SERC's Mitigation Plan required SERC to:

1. complete a formal review of all the firewall rules at all access points to the ESPs and update or remove any old rules that were not needed; and
2. track firewall rule changes through its current change management process to prevent future recurrence.

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

1. a step-by-step firewall review process document for use in determining whether a firewall rule is in use;
2. an email indicating that the firewall review process document was complete and where it was stored;
3. an email thread indicating that the final firewall rules had been removed and included a link to where the tracking sheet was stored; and
4. a spreadsheet indicating the justification for each of the firewall rules.

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

CIP-005-1 R4.2 (SERC2011007988)

URE's Mitigation Plan to address its violation of CIP-005-1 R4.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to revise the existing CVA procedure to state clearly that a review of ports and services allowed through the access points will be reviewed pursuant to CIP-005 R4.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted an updated annual CVA process document that includes language requiring the review of ports and services enabled at the ESP access points and firewall access control lists at least annually in order to ensure intended continuing business purpose.

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

CIP-006-1 R1.7 and R1.8 (SERC2011007989)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.7 and R1.8 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan requires URE to:

1. update a PSP diagram to reflect the reconfiguration of the boundary of an access point for one location;
2. identify all card access system workstations and system panels that authorize and/or log access to PSPs and create a list of these devices;
3. evaluate different options to put the appropriate card access system workstations, servers, and panels behind electronic access points to meet the requirements of CIP-005 R2 and R3;
4. evaluate different options to move the appropriate card access system workstations and panels to meet compliance with the applicable physical security requirements of CIP-006;
5. move the card access system panels and workstations, as necessary, into a physically protected area and develop associated documentation for these assets;
6. purchase and set up the new card access system servers. URE will install new software and test the new servers;

7. place the card access system workstations, servers, and panels behind an electronic access point to meet the requirements of CIP-005 R2 and R3;
8. draft new CIP procedures or revisions to current CIP procedures to address the requirements of CIP-005 R2 and R3 regarding the access points for the card access systems assets;
9. evaluate the passwords on the card access system assets to determine which passwords could be changed annually and determine password policies for the card access system assets;
10. change, based on the results of the password evaluation, the user account structure and setup passwords on the new card access assets that can be changed annually;
11. draft new CIP procedures or revisions to the existing procedures to address CIP compliance for the card access system assets, including addressing the testing of antivirus and malware prevention signatures;
12. work with URE's card access system vendor to change the default account passwords on the card access system assets and document how to change the password annually in the future. If any default account password cannot be changed, confirmation from the vendor will be documented;
13. put into production the new card access system servers and move workstation connections to the new servers;
14. finalize new or revised CIP procedures to address the requirements of CIP-005 R2 and R3 regarding the electronic access points for the card access systems assets;
15. finalize the new or revised CIP procedures for the card access system assets, including addressing testing of antivirus and malware prevention signatures; and
16. file any necessary TFEs with SERC for the card access system assets.

This Mitigation Plan is scheduled for future completion.

CIP-007-1 R2.2 (SERC2011007990)

URE's Mitigation Plan to address its violation of CIP-007-1 R2.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. disable remote access for several CCA devices in favor of using serial interface connections for local management;

2. verify the justification for the remaining CCA devices that remote access was needed for normal and emergency operations; and
3. perform a formal review of the ports and services for the CCA that was identified during the Compliance Audit and verify that these ports and services were needed for normal and emergency operations.

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

1. documents showing before and after port scans for the CCAs that are referenced in the summary report, demonstrating that the four remote access ports were disabled;
2. an attestation certifying that the ports and services on several CCAs identified during the Compliance Audit are needed for normal and emergency operations; and
3. a summary report of a formal review of the ports and services for one CCA that was conducted by a third party.

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

CIP-007-1 R8.3 (SERC2011007992)

URE's Mitigation Plan to address its violation of CIP-007-1 R8.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to revise its existing CVA process to state clearly that default application accounts will be reviewed pursuant to CIP-007 R8.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a revised CVA process that requires the individuals conducting a CVA to review the controls for default application accounts on all Cyber Assets within the ESP at least annually. The revised process also requires assessments to be documented with remediation or mitigation plans.

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

CIP-007-1 R1 (SERC2011007993)

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

URE's Mitigation Plan required URE to revise its CIP-007 R1 test procedure to define more clearly a test plan to verify that significant changes, including the implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware to the applicable CCA do not adversely affect existing cyber security controls.

URE certified that the above Mitigation Plan requirements were completed. As evidence of completion of its Mitigation Plan, URE submitted a revised CIP-007 R1 test procedure that: (i) includes language requiring that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls; and (ii) requires cyber security testing of software upgrades in order to ensure that cyber security controls are not impacted. The review procedure includes lists of the tests or tasks to be performed.

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

CIP-006-3c R2.2 (SERC2012010331)

URE's Mitigation Plan to address its violation of CIP-006-3c R2.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. increase the memory size on the logging system to prevent the logging system from running out of memory in the future;
2. add an alert that notifies the vendor managing the logging system when there is a memory error on the logging system so that the vendor can notify URE of the failure and alternative actions can be taken to send out alerts; and
3. update the alerting procedure that outlines what actions are needed when the alerting process for the PACS servers fails.

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

1. an email identifying the issue of alerts going into an disabled state and noting the solution of making configuration changes to increase memory size;
2. a ticket report that includes a discussion thread regarding the memory issue and noting that the problem had been fixed;
3. an updated security status monitoring procedure that documents the process to follow and tasks to perform if the logging system fails; and
4. an email to URE staff advising them of the need to reprocess system logs if the logging system fails. The updated security status monitoring procedure was attached to the email.

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

CIP-004-3 R2.1 (SERC2012011169)

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

URE's Mitigation Plan required URE to:

1. revoke electronic access from the individual who was granted electronic access without having completed the cyber security training;
2. revise the current procedure for electronic access control to add an additional step for a CIP compliance specialist to verify and document that training and a PRA had been completed prior to granting access to a CCA device; and
3. re-train the personnel responsible for granting access to any CCA device.

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

1. a revised procedure for electronic access control that has specific language stating that the security staff will verify that the PRA and cyber security training are completed and current before sending to the business group responsible for enabling the access;
2. a training attendance record showing that each of the signatories attests that they have read and understand the revised procedure for electronic access control; and
3. a computerized list of over a dozen individuals, including the individuals mentioned previously, who have taken a NERC CIP training course online.

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

CIP-006-3c R1.6 (SERC2013012004)

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

URE's Mitigation Plan required URE to:

1. re-train the contract and employee personnel on the requirements of CIP-004 R2, including providing instructions for escorting personnel in a PSP;
2. assign a specific crew of contract personnel to clean the PSPs involved in this violation and gave them unescorted access privileges after confirming their PRA and cyber security training;
    a. instruct these personnel not to escort anyone into the PSP; and implement a practice that the non-supervisor cleaning crew members must leave their badge with security at the end of each shift; and
3. develop and implement a plan for future cleanings of areas within PSPs.

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

1. an email thread showing the training record of the contract and employee personnel who were retrained on CIP-004 R2 and the instructions for escorting personnel in a PSP;
2. an email thread showing that the contract personnel would access the PSPs on their own and will cooperate with the guidelines for the PSPs; an email thread indicating that the contractor must notify URE immediately when contractor personnel are terminated or transferred to another URE facility, that contractor personnel should never escort anyone into a PSP, and that all contractor personnel with PSP access will turn in their badges at the alarm center at the end of their shift; an email thread showing that the contractor agreed to the policy outlined in the email from URE; and a training spreadsheet showing that all involved individuals had received cyber security training and PRAs; and
3. a document regarding the cleaning crew plan, which states that for PSPs the cleaning crew will be escorted by an URE employee or physical security; and an email thread stating that physical security has been asked to remove unescorted physical access to PSPs for several contractor employees and that the request had been completed.

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

CIP-007-1 R3 (SERC2013012236)

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

URE's Mitigation Plan requires URE to:

1. develop and finalize a list of installed applications and/or software on the new EACM devices to use in the revised patch management program;
2. develop and finalize a list of installed applications and/or software on CCAs to use in the revised patch management program;
3. develop and finalize a list of installed applications/software on the new PAC devices to use in the revised patch management program; and
4. revise and implement a revised patch management program that includes manual steps for checking for available security application patches based on the applications and/or software list created in steps 1 through 3 above.

URE's Mitigation Plan is scheduled for future completion.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[6]

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[7] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a one hundred and twenty thousand dollar ($120,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In

[6] *See* 18 C.F.R. § 39.7(d)(4).

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

approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported several of the violations, as described above;
3. SERC reported that URE was cooperative throughout the compliance enforcement process;
4. URE had a compliance program at the time of the violations which SERC considered a mitigating factor, as discussed above;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SERC determined that 17 of the 19 violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. 2 of the 19 violations posed a serious or substantial risk to the reliability of the BPS, as discussed above;
8. URE has undertaken actions to unify its CIP procedures across departments, restructure its physical security organization, and implement controls and crosschecks to ensure future compliance, which SERC considered a mitigating factor, as discussed above;
9. URE has expended substantial resources to improve compliance and to implement mitigation action to correct violations, which SERC considered a mitigating factor, as discussed above; and
10. SERC reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred and 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

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 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	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 Marisa A. Sifontes* General Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org

Andrea B. Koch* Director of Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org *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.	James M. McGrane* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: SERC Reliability Corporation