December 30, 2013

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

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

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] of CIP-002-1 R3; CIP-003-1 R1 and R4 through R6; CIP-003-3 R6; CIP-004-1 R1 through R4; CIP-004-3 R3; CIP-005-1 R1 through R3 and R5; CIP-005-3a R2; CIP-006-1 R1; CIP-006-3c R1 and R8; CIP-007-1 R1 through R3, R5, and R6; CIP-007-3a R5; CIP-008-1 R1; and CIP-009-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of fifty thousand dollars ($50,000), 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

[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.

Violation Tracking Identification Numbers SERC200900414, SERC200900415, SERC201000665, SERC201000666, SERC201000667, SERC2012010852, SERC201000507, SERC200900416, SERC200900417, SERC2011007656, SERC200900419, SERC201000668, SERC201000669, SERC201000670, SERC2012010853, SERC201000671, SERC2012010854, SERC200900418, SERC201000672, SERC2012010857, SERC201000673, SERC2013012192, SERC2012010637, SERC2012010855, SERC2012009690, SERC2012010856, SERC201000674, SERC201000675, SERC201000676, SERC2012010859, SERC2011007657, SERC2012010858, SERC200900420, and SERC201000677 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

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

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	Unidentified Registered Entity	NOC-2241	SERC200900414	CIP-002-1	R3	High	$50,000
			SERC200900415	CIP-003-1	R1; R1.2	Lower	
			SERC201000665	CIP-003-1	R4	Medium	
			SERC201000666	CIP-003-1	R5	Lower	
			SERC201000667	CIP-003-1	R6	Lower	
			SERC2012010852	CIP-003-3	R6	Lower	
			SERC201000507	CIP-004-1	R1	Lower	

SERC Reliability Corporation	Unidentified Registered Entity	NOC-2241	SERC200900416	CIP-004-1	R2; R2.1	Medium	$50,000
			SERC200900417	CIP-004-1	R3	Medium	
			SERC2011007656	CIP-004-3	R3; R3.2	Lower	
			SERC200900419	CIP-004-1	R4	Lower	
			SERC201000668	CIP-004-1	R4	Lower	
			SERC201000669	CIP-005-1	R1; R1.1; R1.4	Medium	
			SERC201000670	CIP-005-1	R1; R1.5	Medium	
			SERC2012010853	CIP-005-1	R1; R1.5	Medium	
			SERC201000671	CIP-005-1	R2; R2.2	Medium	
			SERC2012010854	CIP-005-3a	R2; R2.2	Medium	
			SERC200900418	CIP-005-1	R2; R2.5.2	Lower	
			SERC201000672	CIP-005-1	R3	Medium	
			SERC2012010857	CIP-005-1	R3; R3.2	Medium	
			SERC201000673	CIP-005-1	R5; R5.1	Lower	
			SERC2013012192	CIP-006-3c	R1; R1.6	Medium	
			SERC2012010637	CIP-006-1	R1; R1.8	Lower	

SERC Reliability Corporation	Unidentified Registered Entity	NOC-2241	SERC2012010855	CIP-006-1	R1; R1.8	Lower	$50,000
			SERC2012009690	CIP-006-3c	R8; R8.1	Medium	
			SERC2012010856	CIP-007-1	R1; R1.3	Lower	
			SERC201000674	CIP-007-1	R2	Medium	
			SERC201000675	CIP-007-1	R3	Lower	
			SERC201000676	CIP-007-1	R5	Lower	
			SERC2012010859	CIP-007-1	R5; R5.2.3; R5.3	Lower	
			SERC2011007657	CIP-007-3a	R5; R5.3.3	Medium	
			SERC2012010858	CIP-007-1	R6; R6.3	Medium	
			SERC200900420	CIP-008-1	R1	Lower	
			SERC201000677	CIP-009-1	R1	Medium	

CIP-002-1 R3 (SERC200900414)

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part:

> Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

CIP-002-1 R3 provides:

> R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:
>
> > R3.1. The Cyber Asset uses a routable protocol to communicate outside the Electronic Security Perimeter; or,
> >
> > R3.2. The Cyber Asset uses a routable protocol within a control center; or,
> >
> > R3.3. The Cyber Asset is dial-up accessible.

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

During a Spot Check, SERC determined that URE was in violation of CIP-002-1 R3. Specifically, URE failed to identify an energy management system (EMS) console with supervisory controls over bulk electric system assets as a Critical Cyber Asset (CCA). This console was located outside of a Physical Security Perimeter (PSP) and was used to troubleshoot remote terminal units. In addition, URE failed to identify its six network switches within the Electronic Security Perimeter (ESP) as CCAs.

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 bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, URE's failure to identify all CCAs could leave those devices without the protections required by the CIP Standards, which could allow a malicious individual to disrupt or disable CCAs. The risk to the reliability of the BPS was mitigated by the following factors. URE's EMS console was connected to the ESP via a private, restricted demilitarized zone (DMZ). The DMZ switch was inside the PSP and programmed to shut down if any

internet protocol (IP) address other than those approved were plugged into it. The firewall was programmed to block interactive access to internal devices using services such as remote desktop, telnet, secure shell, or file transfer protocol. Finally, the network switches were protected within an ESP and PSP.

CIP-003-1 R1; R1.2 (SERC200900415)

The purpose statement of Reliability Standard CIP-003-1 provides in pertinent part: "Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-003-1 R1 provides in pertinent part:

> R1. Cyber Security Policy — The Responsible Entity shall document and implement a cyber security policy that represents management's commitment and ability to secure its Critical Cyber Assets. The Responsible Entity shall, at minimum, ensure the following:
>
> > R1.2. The cyber security policy is readily available to all personnel who have access to, or are responsible for, Critical Cyber Assets.

CIP-003-1 R1.2 has a "Lower" VRF and a "Severe" VSL.

During the Spot Check, SERC determined that URE had a violation of CIP-003-1 R1.2. Specifically, URE was unable to provide evidence that the cyber security policy (CSP) was readily available to all personnel who had access to, or were responsible for, CCAs. URE was unable to provide evidence that the CSP was available to vendors with access 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 made the CSP readily available to vendors with access to CCAs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The violation involved a small number of vendor personnel who had access to CCAs and had been specifically authorized for such access. URE's CSP was readily available to all employees and contractors with URE network access, and the CSP was available in hard copy at all doors providing access to URE PSPs.

CIP-003-1 R4 (SERC201000665)
CIP-003-1 R4 provides:

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

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-003-1 R4. Specifically, URE did not adequately implement a program to identify, classify, and protect information associated with CCAs. An outside consultant assessed URE's documented information protection program and found it to be deficient. The outside consultant identified several documents that contained CCA information but were not appropriately labeled pursuant to URE's information protection program.

SERC determined the duration of the violation to be the date the Standard became mandatory and enforceable on URE through when URE implemented its new information protection program.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement its information protection program by appropriately labeling all documents with CCA information could have led to CCA information being shared with personnel who were not authorized for access to such information. The

risk to the reliability of the BPS was mitigated by the following factors. URE appropriately labeled 79.5% of its documents that had CCA information. URE maintained all identified CCA information documents in PSPs or network shares available only to authorized personnel. Also, a single URE subject matter expert (SME) was responsible for managing and authorizing access to all CCA information, reducing the chance that an unauthorized individual would be able to gain access to CCA information.

CIP-003-1 R5 (SERC201000666)

CIP-003-1 R5 provides:

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

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-003-1 R5. Specifically, URE failed to implement a program adequately for managing access to protected CCA information. URE's program for managing access to protected CCA information identified a single individual who was authorized to approve logical or physical access to CCA information and included the identifying information required by R5.1.1. The program also called for annual reviews or assessments as required

by R5.1.2, R5.2, and R5.3. However, URE was unable to provide any documentation showing that it: 1) verified the list of personnel responsible for authorizing access to CCA information annually, as required by R5.1.2; 2) annually reviewed the access privileges to CCA information, as required by R5.2; or 3) annually assessed and documented the processes for controlling access privileges to CCA information as required by R5.3.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE implemented its new information protection program.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement its program for managing access to protected CCA information could have led to CCA information being shared with personnel who were not authorized for access to such information. The risk to the reliability of the BPS was mitigated by the following factors. URE maintained all identified CCA information documents in PSPs or network shares available only to authorized personnel. Also, a single URE SME was responsible for managing and authorizing access to all CCA information, reducing the chance that an unauthorized individual would be able to gain access to CCA information.

CIP-003-1 R6 (SERC201000667)

CIP-003-1 R6 provides:

> Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-1 R6 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-003-1 R6. Specifically, URE did not follow its change management procedure when replacing certain hardware. URE hired an outside consultant to review, identify, and remediate deficiencies in its CIP program for a specific year. During this review, URE identified a few instances when it removed Cyber Assets within the ESP after it made the decision not to make any significant changes. URE was unable to provide records showing that it followed its change management process when removing the Cyber Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE implemented new change control and configuration management procedures.

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 follow a process of change control and configuration management could have allowed unauthorized changes to occur without proper understanding and review of the potential impacts to operations and the BPS. The risk to the reliability of the BPS was mitigated by the following factors. The changes URE made to Cyber Assets within the ESP during the violation involved the removal or decommissioning of Cyber Assets, as opposed to the addition of Cyber Assets. URE followed its CIP-007 disposal procedures and documented the sanitization of the Cyber Assets when it removed those Cyber Assets from service.

CIP-003-3 R6 (SERC2012010852)

The purpose statement of Reliability Standard CIP-003-3 provides: "Standard CIP-003-3 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-003-3 R6 provides:

> Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor-related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

CIP-003-3 R6 has a "Lower" VRF and a "Severe" VSL.

During a Compliance Audit, SERC determined that URE was in violation of CIP-003-1 R6. Specifically, URE failed to follow its established change control and configuration management procedures. SERC later determined that URE was in violation of CIP-003-3 R6. URE failed to complete applicable change management forms for the major upgrade of its EMS. URE's change management policy was designed to initiate additional processes to create configuration management data (CMD), which would be recorded on a CMD data sheet. However, in this case, the EMS vendor provided URE with the

information that would normally be entered on the CMD data sheets. As a result, URE did not complete the forms specified in its documented process for every device being changed.

SERC determined the duration of the violation to be from when URE replaced its EMS through when URE completed training for its newly created CIP processes and procedures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE completely replaced its EMS and used a single change control and configuration management form to document the collective changes. URE received new baseline configurations for all altered Cyber Assets from the vendor implementing the EMS change. The new EMS was thoroughly tested on the factory floor and after delivery, including cyber security testing and the establishment of the baseline security profiles. URE used its CIP-007 redeployment and disposal procedures when disposing of the old EMS assets.

CIP-004-1 R1 (SERC201000507)

The purpose statement of Reliability Standard CIP-004-1 provides: "Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-004-1 R1 provides:

> Awareness — The Responsible Entity shall establish, maintain, and document a security awareness program to ensure personnel having authorized cyber or authorized unescorted physical access receive on-going reinforcement in sound security practices. The program shall include security awareness reinforcement on at least a quarterly basis using mechanisms such as:
>
> - Direct communications (e.g., emails, memos, computer based training, etc.);
> - Indirect communications (e.g., posters, intranet, brochures, etc.); and
> - Management support and reinforcement (e.g., presentations, meetings, etc.).

CIP-004-1 R1 has a "Lower" VRF and a "High" VSL.

On March 11, 2010, URE submitted a Self-Report to SERC stating that it was in violation of CIP-004-1 R1. Specifically, URE did not provide security awareness reinforcement on at least a quarterly basis to

vendor employees with cyber access to CCAs. URE had a security awareness program that required the reinforcement of security awareness training for individuals with physical and cyber access to CCAs at least quarterly and provided multiple options that could be utilized to facilitate this reinforcement training. URE placed security awareness training posters inside its PSPs near the entrance door. Several off-site support vendors for its EMS, all with authorized cyber access to CCAs, had never been physically on site, and thus had never been exposed to or seen the security awareness training posters. As a result of this oversight, the affected individuals did not receive the required quarterly security awareness reinforcement.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE sent a cyber security awareness reminder email to the vendor employees.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. This violation impacted 12.8% of the URE's personnel with authorized cyber or physical access to CCAs. All the affected support vendors had current cyber security training and current personnel risk assessments (PRAs). The support vendors worked for the same EMS vendor and were aware of the importance of cyber security to the energy industry.

CIP-004-1 R2; R2.1 (SERC200900416)

CIP-004-1 R2 provides in pertinent part:

> R2. Training — 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 the Spot Check, SERC determined that URE was in violation of CIP-004-1 R2.1. Specifically, URE failed to provide evidence that security training was completed within 90 days of authorization for personnel having authorized cyber or authorized unescorted physical access to CCAs.

URE's cyber security policy specifically required that training be conducted and documented for all personnel with authorized cyber or authorized unescorted physical access to CCAs, but did not specify that the training must occur within 90 days of access being authorized. URE was unable to provide evidence that it provided cyber security training to several of its employees and vendors and contractors within 90 days of granting those individuals access to CCAs. The affected employees were trained several days to weeks after the required 90-day period. In addition, URE failed to record the training dates for the vendors and contractors until over a year after CIP-004-1 R2 became mandatory and enforceable on URE.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE recorded that it provided cyber security training to the last of the vendors with access to CCAs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to provide training to a small number of individuals (13.4%) with authorized cyber or authorized unescorted physical access to CCAs within 90 days of granting them access. All the affected individuals were in good standing with URE prior to and during this violation. All the affected employees are still employed with URE and remain in good standing.

CIP-004-1 R3 (SERC200900417)

CIP-004-1 R3 provides:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:
>
> > R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct

more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

R3.2. The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.

R3.3. The Responsible Entity shall document the results of personnel risk assessments of its personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, and that personnel risk assessments of contractor and service vendor personnel with such access are conducted pursuant to Standard CIP-004.

CIP-004-1 R3 has a "Medium" VRF and a "Severe" VSL.

During the Spot Check, SERC determined that URE was in violation of CIP-004-1 R3. Specifically, URE failed to provide evidence that PRAs for personnel having authorized cyber or authorized unescorted physical access were conducted within 30 days of such personnel being granted such access. URE's cyber security policy specifically required that a PRA be conducted on all personnel with authorized cyber or authorized unescorted physical access, but did not specify that the PRA must be conducted within 30 days of access being granted. For several individuals, consisting of security guards, employees, and contractors, URE conducted PRAs more than 30 days after the individuals were 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 the last PRA for the affected individuals.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to conduct a PRA for a small number of individuals (8.5%) with authorized cyber or authorized unescorted physical access to CCAs within 30 days of granting access. All the affected individuals were in good standing with URE prior to and after this violation. The missed employees and contractors were long-term employees and contractors that remain with URE. All the affected security guards had passed a criminal background check, motor driving record check, and a drug screening prior to being hired by the security company.

CIP-004-3 R3; R3.2 (SERC2011007656)

The purpose statement of Reliability Standard CIP-004-3 provides: "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 R3 provides in pertinent part:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.
>
> The personnel risk assessment program shall at a minimum include:
>
> ***
>
> R3.2 The Responsible Entity shall update each personnel risk assessment at least every seven years after the initial personnel risk assessment or for cause.
>
> ***

CIP-004-3 R3.2 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-004-3 R3.2. Specifically, URE failed to update PRAs for a few employees within seven years as required. URE maintained an access program and used it to track PRA completion dates and alert the user when PRA renewals were coming due within the next year. URE began using a new manual process for reviewing and performing PRA updates and changed the person responsible for performing those updates. As a result of these changes, URE overlooked the required seven-year PRA renewal for the affected employees. URE did not conduct a new PRA for the affected employee prior to the expiration of the existing PRAs. URE discovered this violation during an internal access program assessment and immediately revoked the CCA access rights for the affected employees pending the results of their PRA renewals.

SERC determined the duration of the violation to be from when the first employee's PRA expired without being renewed through when URE revoked access to CCAs for the affected employees.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE revoked the employees' access to CCAs within a short period of time after the expiration of the employees' previous PRAs. The affected employees were in good standing with URE prior to the lapse in their PRAs and remained in good standing after URE discovered this violation. The affected employees were current in their cyber security training.

CIP-004-1 R4 (SERC200900419)

CIP-004-1 R4 provides:

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

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

During the Spot Check, SERC determined that URE was in violation of CIP-004-1 R4. Specifically, URE could not provide evidence that it maintained lists of personnel with authorized cyber or authorized unescorted physical access to CCAs, including their specific electronic and physical access rights to CCAs. URE also granted personnel unescorted physical access using temporary access cards without properly documented authorization.

URE maintained three CCA access lists. URE maintained one physical CCA access list for the primary control center (PCC) and one for the back-up control center (BCC). URE reviewed each of these lists quarterly and updated them as required. URE also reviewed the electronic CCA access list quarterly and updated it as required. URE's electronic CCA access list did not contain specific access rights to CCAs because the individuals that had electronic access had access to all CCAs, not just subsets or

groupings of CCAs. URE was unable to show specific access rights for the individuals with authorized electronic access to CCAs. The violation affected 30.5% of total individuals with authorized cyber or authorized unescorted physical access to CCAs.

URE also granted an individual, using a temporary access card, unescorted physical access without properly documented authorization. URE had a master access card that was kept in a lock box in the PCC PSP. This card could originally open every door in the headquarters building, including the PSP doors for the PCC. It was available in case an authorized user forgot their access card or in the case of an emergency. One individual obtained this card on a few separate occasions from the system operators without first obtaining authorization for unescorted physical access to the URE PSPs.

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 URE personnel were included on CCA access lists. The affected individuals with electronic access did not have their specific access rights documented. URE's SME was aware of the individuals who should have electronic access to CCAs and was aware of their specific access rights. The employee who obtained the master access card was a long-term custodial contract supervisor who was and still remains in good standing with URE.

CIP-004-1 R4 (SERC201000668)

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-004-1 R4. Specifically, URE did not include the specific electronic access rights for personnel that could electronically access a CCA while within the PSP using their authorized unescorted physical access to the PSP. URE's CCA access list did not include the specific electronic access rights for 47% of individuals with authorized cyber or authorized unescorted physical access to CCAs who had approved unescorted physical access to PSPs and could also log in and use CCAs while within the PSP.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE created a new CCA access list that included all personnel and their specific electronic and physical access rights.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Despite URE's failure to document each individual's specific physical or electronic access

rights, all personnel with authorized cyber or authorized unescorted physical access to CCAs were accounted for on the URE list. URE had valid PRAs and completed annual cyber security training for all affected personnel that could log-in and use CCAs while within the PSP. URE followed the appropriate internal approval process for all affected personnel. No unauthorized personnel had access to any CCAs.

CIP-005-1 R1; R1.1 and R1.4 (SERC201000669)

The purpose statement of Reliability Standard CIP-005-1 provides: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 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).
> >
> > ***
> >
> > R1.4. 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 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.4. Specifically, URE failed to identify and protect a few non-critical Cyber Assets within the ESP. On the same day, URE submitted an additional Self-Report to SERC stating that it was in violation of CIP-002-1 R3. Specifically, URE failed to identify a few terminal servers used as serial front end processors to field remote terminal units (RTUs) as CCAs. SERC determined that URE failed to identify the terminal

servers as access points, a violation of CIP-005-1 R1.1, and decided to treat the second Self-Report as an expansion of the scope of the first violation.

URE failed to identify a few Synchronous Optical Networking (SONET) end points as non-critical Cyber Assets within the ESP. URE originally set up a single ESP spanning PSPs at its PCC and BCC. The SONET end points provided a communication link between the PCC and BCC for various forms of data to be multiplexed together and transported over the SONET connection using non-routable protocols. The SONET endpoints are physically located inside the PSPs. URE also failed to identify a terminal server as a non-critical Cyber Asset within the ESP. This terminal server was used to update the map board through serial-only communications.

URE had originally identified several additional terminal servers as CCAs. SERC determined that URE was not required to identify these terminal servers as CCAs, but instead should have identified them as access points to the ESP. Later, URE identified the terminal servers as access points. SERC determined that URE was in violation of CIP-005-1 R1.1 because URE originally failed to identify the additional terminal servers as 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 the terminal server used to update the map board was identified and protected as a Cyber Asset in an ESP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The SONET devices were non-routable Cyber Assets and were not identifiable on the network. The terminal server was used to update the map board, which was not connected to any other system or Cyber Assets. In addition, the terminal servers that were misidentified as CCAs received all the protections afforded to CCAs.

CIP-005-1 R1; R1.5 (SERC201000670)

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).

***

R1.5. 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 R1.5 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R1.5. Specifically, URE failed to afford a Cyber Asset the protective measures specified in R1.5. URE submitted a second Self-Report to SERC stating that it was in violation of CIP-007-2a R5.3.3 because it discovered it did not annually change passwords on several shared accounts for a few firewalls. SERC determined that this portion of the violation was more appropriately addressed as a failure to afford Cyber Assets used in the electronic access control and monitoring of the ESP the protective measures specified in CIP-007 R5.3.3, a violation of CIP-005-1 R1.5.

SERC determined that URE had two incidents when it was not in compliance with CIP-005-1 R1.5. In the first incident, URE failed to identify a Cyber Asset used to authenticate remote access into the ESP as an electronic access control and monitoring (EACM) device. This Cyber Asset was a virtual private network (VPN) termination point, and resided within the PSP, but outside of the ESP firewall which served as the access point. Because it failed to identify the Cyber Asset as an EACM device, URE was unable to provide evidence that it had afforded the Cyber Asset the protections listed in CIP-005-1 R1.5.

In the second incident, URE discovered during an internal access program assessment that it did not annually change passwords on several shared accounts for a few firewalls. URE had inadequate alerts and notifications in place to remind administrators to change the passwords annually. Previously, URE had depended on the annual reviews of access and shared accounts to be the triggers for the administrators to change the passwords. However, because the annual review process lacked specific direction and guidance, URE failed to change passwords for the shared accounts on the firewalls for a specific year. After discovering the violation, URE immediately changed the affected shared account passwords. SERC determined that URE was in violation of CIP-005-1 R1.5 because it failed to provide EACM devices the protective measures specified in CIP-007-1 R5.3.3.

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 firewall 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 provide the protective measures listed in CIP-005 R1.5 to its EACM devices could allow unauthorized personnel to gain access to CCAs, potentially disrupting URE's visibility or control over its portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. The VPN termination point was secured within an established PSP. While the firewall passwords were not changed annually, they did meet the complexity requirements of CIP-007-1 R5.3.

CIP-005-1 R1; R1.5 (SERC2012010853)

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

During the Compliance Audit, SERC determined that URE was in violation of CIP-005-1 R1.5. Specifically, URE failed to afford Cyber Assets used in the electronic access control and monitoring of the ESP the protective measures specified in CIP-003-1 R6 and CIP-007-1 R1.3. URE failed to follow its established change control and configuration management procedures for all Cyber Assets used in the electronic access control and monitoring of the ESP (EACM devices) and failed to document the test results adequately. URE did not obtain a signature indicating that URE personnel had confirmed that configuration profiles had been updated, as required in URE's documented procedure for changes to EACM devices. The change had been properly approved. When testing the change, URE only documented that the EACM device passed the cyber security testing, and did not record additional information. URE was unable to provide evidence of an established change control and configuration management process prior to when it implemented an interim change control form. At a later date, URE implemented a full change control and configuration management process that included EACM devices.

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 change control procedures to address changes to EACM devices and updated its cyber security testing procedures to include the retention of test plans.

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, improperly documenting the cyber security testing for significant changes could result in changes to EACM devices that were not properly authorized, documented, or tested and could leave URE personnel without knowledge that the changes had

occurred. The risk to the reliability of the BPS was mitigated by the following factors. There was one significant change to EACM devices during the violation, which had been approved. URE performed testing for significant changes on the change and documented that it passed cyber security testing. Finally, the EACM device was protected within a PSP.

CIP-005-1 R2; R2.2 (SERC201000671)

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.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R2.2. URE had not: 1) properly documented the reasons for open ports; 2) approved some changes; and 3) implemented some changes as approved. In addition, URE had not completed all of the proper forms, lists, and records required in the URE procedures.

During a vulnerability assessment, URE discovered it had enabled ports and services that were not properly documented on a few firewalls that served as access points to its ESP. URE also found that some changes to ports and services had not been properly approved or were not implemented as approved. In addition, URE documented the need for certain ports and services within the rules on the firewalls, but did not maintain a baseline document that was separate from the firewall rules and did not document the reasons why these communications were permitted.

URE also found several firewall rules that had been approved but were not implemented as specified. One change that was approved called for URE to allow inter-control center communications protocol (ICCP) and internet control message protocol (ICMP) communication from a neighboring utility from outside the firewall to a specific set of servers and also called for URE to close one ICCP port and ICMP to several IP addresses that the neighboring utility no longer used. While the firewall rule change was implemented for operational functionality, URE failed to limit communication from the neighboring utility to the specified servers and instead allowed communication from the neighboring utility via ICCP and ICMP to any Cyber Asset within the ESP. URE also failed to close the one ICCP port and ICMP on half of the IP addresses that were no longer in use.

Furthermore, URE implemented a remote access request to an additional CCA workstation without receiving or approving an access request form. URE had previously approved the same type of access for several other workstations. To reach these workstations, users first had to establish a virtual VPN connection to another firewall outside of the ESP.

Finally, URE submitted and approved an access request form to permit outbound email from a CCA to an email server outside the ESP. When URE was about to create the firewall rule, it found that the rule already existed on the firewall rule set and had been undocumented since before CIP-005 R2 became mandatory and enforceable.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE properly documented the ports and services required for operations and for monitoring Cyber Assets within the ESP and closed all unnecessary ports and services.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE failed on several occasions to implement and document organizational processes and technical and procedural mechanisms for control of electronic access at the ESP. URE failed to: 1) document properly the reasons some ports and services were enabled on firewalls; 2) implement approved changes to firewall rules; and 3) document previously implemented firewall rules. In addition, URE implemented unapproved changes to firewall rules. These failures could allow an unauthorized individual to gain access to and control of CCAs, potentially leading to a loss of control or visibility over URE's portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. Exploitation of the open ICCP port or ICMP allowing communication with the neighboring utility would require gaining access to the neighboring entity's Cyber Assets. Even though the firewall allowed communication on the ICCP port and ICMP to pass into the ESP, the other Cyber Assets within the ESP were not configured to respond to ICCP traffic. The unapproved

changes were made by an SME who was responsible for determining whether the changed firewall rules were appropriate before seeking approval by another manager.

CIP-005-3a R2; R2.2 (SERC2012010854)

The purpose statement of Reliability Standard CIP-005-3a provides: "Standard CIP-005-3 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-005-3a 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-005-3a R2.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC determined that URE was in violation of CIP-005-3 R2.2. Specifically, URE failed to enable only ports and services at electronic access points to the ESP that were required for operations and for monitoring Cyber Assets within the ESP. At the time of the Compliance Audit, URE had a process in place that required it to document the ports and services required for each Cyber Asset to function properly, and then disable all other ports and services. It had a similar process in place for access points that required it to identify and document the required ports services through the access points. This process included steps to ensure logging and alerting for these access points was enabled and establish account authentication.

However, based on the recommendations of the EMS vendor, URE did not follow its established processes. Instead, URE established firewall rules that were overly permissive and allowed ports to be

enabled beyond what was required for operations and for monitoring Cyber Assets within the ESP. URE had several inbound ports and numerous outbound ports, with a few of these ports communicating from one ESP to another ESP, that were enabled but were not required for operations or monitoring Cyber Assets within the ESP.

SERC determined the duration of the violation to be from when URE's new EMS with the new firewalls were commissioned with more permissive rules, through when URE implemented more restrictive access control rules with the deployment of new EMS firewalls.

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 open ports and services that were not required for normal or emergency operations could allow a malicious individual to gain access to and control of CCAs, potentially leading to a loss of control or visibility over URE's portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. The majority of the ports that should not have been enabled were outbound ports and would not allow an outsider through the ESP. URE had established a corporate firewall between the ESP firewall and any internet access, which reduced the chance that an outsider could make use of the enabled inbound ports.

CIP-005-1 R2; R2.5.2 (SERC200900418)
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).
>
> ***
>
> R2.5. The required documentation shall, at least, identify and describe:
>
> ***
>
> R2.5.2. The authentication methods.

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

During the Spot Check, SERC determined that URE was in violation of CIP-005-1 R2.4. Specifically, URE failed to provide evidence that it had implemented strong procedural or technical controls at access points to authenticate the accessing party where external interactive access is permitted into the ESP. SERC later determined that the violation was more appropriately addressed as a failure to document the authentication methods used to ensure the authenticity of the accessing party where external interactive access into the ESP was enabled, a violation of CIP-005-1 R2.5.2.

URE's electronic access procedure did not provide in-depth details about how the strong procedural or technical controls were established and deployed for ensuring the authenticity of an accessing party making use of external interactive access into the ESP. Instead of fully documenting these controls, URE depended on the experience and knowledge of a single SME to implement strong procedural or technical controls to authenticate the accessing party where external interactive access into the ESP was enabled.

URE allowed three types of remote interactive access into the ESP. All connections over the Internet were via encrypted VPNs.

First, a few consoles outside the ESP were connected to a private restricted DMZ that connected directly to the ESP firewall. The DMZ switch was inside the PSP and programmed to shut down the affected port if any IP address other than those approved was plugged into it. The EMS software was configured to allow only the most restrictive permission held by the user and workstation. The firewall was programmed to block interactive access to Cyber Assets within the ESP.

Second, authorized URE employees could connect through the ESP from home via VPN. Employees would use the VPN to connect to a firewall outside of the ESP. Each employee had unique passwords allowing for identification. After making the connection, the employee would initiate a remote desktop session from their home computer to their EMS workstation, where they had to login again using their normal EMS domain credentials.

Finally, authorized EMS vendor personnel could connect from the remote vendor office. URE had established a permanent firewall-to-firewall VPN with the EMS vendor that terminated at a firewall outside the ESP. This VPN had a complex shared key, and no other IP address was permitted to use it. Rules in the external firewall and the ESP firewall forced the sessions from the EMS vendor to a single internal server. Each of the authorized EMS vendor employees had their own login ID on this server.

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 document the authentication methods meant that URE relied entirely on a single URE SME to manage the process of authenticating accessing parties. The risk to the reliability of the BPS was mitigated by the following factors. URE had several authentication methods that it used to authenticate the external party attempting to access devices within the ESP. The SME had a team of professionals who could continue to maintain the authentication system that URE used.

CIP-005-1 R3 (SERC201000672)

CIP-005-1 R3 provides:

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

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R3. URE failed to document properly all electronic or manual processes for monitoring and logging access at access points to the ESP 24 hours a day, seven days a week. URE failed to document the processes that were being used to monitor and log access at a few access points to the ESP, specifically primary and backup firewalls. Although URE attested that it had implemented an automated system to perform the logging for the firewalls that were in place prior to the date of mandatory compliance, it had no documentation on how this process worked. URE was able to provide an automated email alert showing an authorized remote access attempt by a support vendor to one of the URE firewalls. URE

was unable to provide additional logs because the firewalls at issue were replaced during a subsequent system design. URE created a documented process for setting up either automated or manual monitoring and logging of access at 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 documented the process for monitoring and logging access at the access points to the ESP.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE logged and monitored access at the access points to the ESP using an automated tool which was protected within a PSP and ESP. URE only failed to document the process being used for monitoring and logging.

CIP-005-1 R3; R3.2 (SERC2012010857)
CIP-005-1 R3.2 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SERC determined that URE was in violation of CIP-005-1 R3.2. Specifically, URE failed to submit technical feasibility exceptions (TFEs) for its technical inability to detect and alert for attempted or actual unauthorized access at two types of access points.

URE had a process for monitoring and logging on all Cyber Assets which detailed how URE would accomplish automated monitoring of logs where technically feasible. If automated monitoring of logs was not technically feasible, the process described how URE would conduct and document manual reviews and respond to the reviews on a monthly basis. URE had several terminal server access points and one firewall configured without an IP address that only allowed traffic to flow out of the ESP to a quality assurance system.

Based on URE's network drawing, the terminal servers were ESP border devices, and URE identified them as non-routable ESP access points. These terminal servers connected to remote terminal unit (RTU) modems outside of the ESP using non-routable and non-dial-up serial connections which allowed the terminal servers to obtain RTU supervisory control and data acquisition (SCADA) data from remote substations. URE did not believe it was required to establish logging for serial devices. URE also conducted monthly manual reviews of the logs associated with all its terminal servers and documented the results. URE did not request a TFE for the terminal servers.

The firewall was also identified on the URE network drawing as a non-routable ESP access point. URE configured this firewall without an IP address and the firewall only allowed traffic to flow out of the

ESP (via a mirrored port configured to permit only egress traffic) to a quality assurance system URE used to test any changes using live data. Because URE configured the firewall not to permit any inbound traffic from outside the ESP, it did not provide the ability to alert upon unsuccessful unauthorized access attempts. SERC confirmed that the firewall did not provide the ability to alert on unsuccessful unauthorized access attempts because of the way it was configured. URE did not submit a TFE for logging and did not conduct a manual review of logs because the firewall was not permitted to receive any inbound traffic.

SERC determined the duration of the violation to be from when URE commissioned these access points, through when URE submitted TFEs with SERC that addressed its inability to log and alert electronically for attempts at or actual unauthorized accesses.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE manually logged and reviewed the access logs for the terminal servers on a monthly basis. URE did not find any unauthorized access attempts during its reviews of the access logs. The terminal servers connected to the RTUs did not utilize any routable or dial-up access. The firewall was configured without an IP address and only allowed traffic to flow out of the ESP via a mirrored port configured to permit only egress traffic. The firewall logs only contained denied traffic.

CIP-005-1 R5; R5.1 (SERC201000673)

CIP-005-1 R5 provides in pertinent part:

> R5. Documentation Review and Maintenance — The Responsible Entity shall review, update, and maintain all documentation to support compliance with the requirements of Standard CIP-005.
>
> > R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005 at least annually.

***

CIP-005-1 R5.1 has “Lower” VRF and a “Severe” VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-005-1 R5.1. URE failed to perform the annual review of documents and procedures referenced in CIP-005-1. URE hired an outside consultant to review its CIP program. As a result of this review, URE learned that it had not

conducted the required annual review for that year of its CIP-005 documentation. URE believed that the annual review was required by a certain date, but URE overlooked the annual review for that year and did not conduct one. URE redesigned its CIP program beginning in the middle of the affected year, and concluded the redesign the following year.

SERC determined the duration of the violation to be from the day after URE should have conducted its annual review of CIP-005 documentation for the affected year, when URE completed its redesign of its CIP-005 program and set up reoccurring calendar reminders for the required documentation reviews.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to have a fully established and functioning program review could have left in place inadequate or deficient processes and procedures that were required to secure the ESP and all CCAs and non-critical Cyber Assets within the ESP. The risk to the reliability of the BPS was mitigated by the following factors. All Cyber Assets were secured within established ESPs that utilized firewalls with deny-by-default rules in place and real-time monitoring and alerting. All ESPs were protected within established PSPs with real-time monitoring and alerting.

CIP-006-3c R1; R1.6 (SERC2013012192)

The purpose statement of Reliability Standard CIP-006-3c provides: "Standard CIP-006-3 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

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 was in violation of CIP-006-3c R1.6. Specifically, URE failed to implement its visitor control program properly. URE had a visitor control program that detailed expectations of how visitors into any PSP should be managed. URE held a retirement celebration for retiring system operators in the PCC that several visitors attended. The visitors were all current or former employees of URE or family members of the retiring system operators. Several days after the event, URE manually reviewed the log book and found that not all of the visitors were properly signed in to the PCC as required. URE personnel properly logged approximately one-third of the visitors in and out of the PCC and recorded the name of their escort. URE personnel properly signed in a few other visitors and recorded the name of their escort, but did not properly sign out the visitors. Finally, URE personnel did not make any visitor log book entries for the other remaining visitors.

As a result of this violation, URE reviewed its visitor logs and discovered that a similar incident occurred during another retirement celebration in the PCC. In this second incident, URE personnel properly logged a visitor, the husband of a retiring URE employee, into the PCC PSP on the visitor log book, but did not properly sign the visitor out. URE did not find any similar violations concerning its PSP for the BCC. As a result of these failures, URE was unable to ensure that it properly escorted and managed visitors while within the PCC PSP.

SERC determined the duration of the violation to be the two dates of the two retirement parties, when URE failed to sign out a visitor of the PCC PSPs, and when URE allowed visitors into the PCC PSP without properly signing them into the logbook.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The PCC was staffed with authorized personnel 24 hours a day, seven days a week. The PCC doors had security cameras which could be used to identify the individuals granted access to the PSP, and URE had security guards at the site of the PCC.

CIP-006-1 R1; R1.8 (SERC2012010637)

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. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 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:
>
> ***
>
> R1.8. 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 R1.8 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-1 R1.8. Specifically, URE failed to afford Cyber Assets used in physical access control and monitoring the protective measures required. URE originally only identified and protected the Physical Access Control Systems (PACS) server as a Cyber Asset used in the access control and monitoring of the PSP. In doing so, URE did not identify two workstations as PACS devices. These workstations were connected to the corporate network and ran administrative client software used to code card readers and change access rights on PSP doors. Additionally, URE failed to identify and protect two control panels for the PSP doors at the PCC and BCC as PACS devices.

One workstation was located outside of the PSP, and the second workstation was inside the PSP, but both were connected to the corporate network. The workstation outside the PSP was within a secured room that only certain employees could access. Of those employees, only one had an account on the workstation that could be used to change the access rights on access badges. The workstation within

the PSP ran read-only administrative software, and personnel could use it to log into the PACS system client software and monitor activity on the card reader access system. The two control panels also resided on the corporate network and could be accessed by the workstations. The control panels were associated with the doors at the PCC, and doors at the BCC but could not be used to change access rights.

After this discovery, URE conducted an internal review of its Cyber Assets used in the access control and monitoring of the PSP and determined that the PACS devices identified above were all the PACS devices associated with its access control and monitoring of the PSP. URE determined that because it failed to identify these Cyber Assets as PACS devices, it failed to provide the PACS devices with any of the protections listed in CIP-006-1 R1.8.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE as a through when URE removed the connection between the corporate network and the PACS workstations and control panels.

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 and protect PACS devices left those PACS devices accessible from the corporate network, which could allow unauthorized individuals to gain access or modify the access rights of existing access badges in order to gain unauthorized access to the PSP. The risk to the reliability of the BPS was mitigated by the following factors. The workstation that resided outside of the PSP was within a secured room to which only one individual had cyber access, and the second workstation was secured physically within a PSP. In addition, the control panels could not be used to change the access rights of access badges.

CIP-006-1 R1; R1.8 (SERC2012010855)
CIP-006-1 R1.8 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SERC determined that URE was in violation of CIP-006-1 R1.8. URE failed to afford its Cyber Assets used in the access control and monitoring of the PSP the protective measures specified in CIP-003 R6 and CIP-007 R1.3. Specifically, URE failed to follow established change control and configuration management procedures for all Cyber Assets used in access control and monitoring of the PSP and failed to document the test results adequately.

For a single change, URE did not obtain a signature indicating that URE personnel had confirmed that the configuration profiles had been updated, as required in URE's documented procedures for changes to PACS devices. The change had been properly approved. In addition, when testing the change, URE

only documented that the PACS device passed the cyber security testing and did not record additional information.

Furthermore, URE was unable to provide any established change control and configuration management process prior to when it implemented an interim change control form. URE implemented a full change control and configuration management process that included PACS devices.

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 change control procedures to address PACS devices and updated its cyber security testing procedures to include the retention of test plans.

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 have a change control and configuration management program and to document properly the cyber security testing for significant changes could result in changes to PACS devices that were not properly authorized, documented, or tested, leaving URE personnel without knowledge that the changes had occurred. The risk to the reliability of the BPS was mitigated by the following factors. The one significant change to PACS devices during the violation was approved. URE performed testing for significant changes on the change and documented that it passed cyber security testing. Also, the PACS device was protected within a PSP and ESP.

CIP-006-3c R8; R8.1 (SERC2012009690)
CIP-006-3c R8 provides in pertinent part:

> R8. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R4, R5, and R6 function properly. The program must include, at a minimum, the following:
>
> > R8.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.

***

CIP-006-3c R8.1 has a "Medium" VRF and a "Severe" VSL.

On February 8, 2012, URE submitted a Self-Report to SERC stating that it was in violation of CIP-006-3c R8.1. URE failed to test physical access control and monitoring (PACM) devices on a cycle no longer than three years, as required. URE tested and implemented the PACM system at its primary energy

control center (ECC) , and at its BCC approximately two years later. The original URE physical security plan called for testing of the PACM system to occur on a cycle not to exceed three years. A couple months after the PACM system was tested and implemented at its BCC, URE revised its physical security plan to require testing of the PACM system on an annual basis. As a result of the change to its physical security plan, URE scheduled PACM system testing at both the ECC and BCC for a year later. URE conducted testing at the ECC and BCC that year. However, URE exceeded the three-year testing and maintenance cycle at the ECC as required by CIP-006-3c R8 by approximately six months. URE conducted testing at the BCC within the required three-year testing and maintenance cycle due to the later PACM implementation date at the BCC.

SERC determined the duration of the violation to be from the day after URE passed the three-year cycle for testing and maintenance of its PACM devices at the ECC through January when URE conducted the required testing of its PACM devices at the ECC.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE staffed its ECC with authorized personnel 24 hours a day, seven days a week. URE designed its physical security system to fail secured in the event of a system or network failure. Although URE tested its PACM devices at the ECC approximately six months after the required three-year testing and maintenance cycle expired, the subsequent test revealed no problems.

CIP-007-1 R1; R1.3 (SERC2012010856)

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). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

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.

***

R1.3. The Responsible Entity shall document test results.

CIP-007-1 R1.3 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SERC determined that URE was in violation of CIP-007-1 R1.3. Specifically, URE failed to document adequately test results of security testing performed for significant changes made. URE had an established testing policy that required URE to conduct testing to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cyber security controls. URE was unable to provide documented cyber security testing procedures prior to for approximately three years after the Standard became mandatory and enforceable on URE. SERC identified several changes to Cyber Assets where URE failed to have test plans and did not retain the test results as evidence. Instead, URE was able to provide the final assessment of the cyber security testing that indicated whether the change either passed or failed. Although the final assessment of the test is indicative of testing being conducted, SERC determined that it was inadequate evidence to demonstrate that URE was testing in a manner that reflected the production environment and was inadequate documentation of the test results. After the Compliance Audit, URE determined that it did not retain the required testing documentation for 57% of its Cyber Assets that had been tested in its CIP program.

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 cyber security testing procedures to include the retention of test plans.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. URE's failure to document and then properly implement cyber security testing procedures could have allowed significant changes to go untested, potentially introducing new vulnerabilities into the affected Cyber Assets. This could lead to unauthorized access to CCAs without the knowledge of URE personnel. The risk to the reliability of the BPS was mitigated by the following factors. Although URE did not retain test plans indicating how the Cyber Assets were tested, URE performed cyber security testing and retained the final result indicating whether the change passed or failed the cyber security testing. URE implemented and tested a small number of significant changes during the violation. Although inadequate as testing documentation, the final assessment of the tests was indicative of testing actually being conducted.

CIP-007-1 R2 (SERC201000674)

CIP-007-1 R2 provides:

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

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R2. Specifically, URE had open ports and services that were not appropriately documented. During a vulnerability assessment conducted, URE discovered ports and services on 64% of its Cyber Assets within the ESP that were enabled but not required for normal or emergency operations. URE had documented processes to ensure that only those ports and services required for normal and emergency operations were enabled but failed to implement those processes successfully.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE conducted a review and created new baselines, and enabled only the ports and services required for normal and emergency operations.

This violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to disable ports on CCAs and non-critical Cyber Assets within the ESP that were not required for normal or emergency operations could have allowed malicious individuals to gain access to and control of CCAs, potentially leading to a loss of control or visibility over URE's portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. All Cyber Assets were within an ESP and a PSP.

CIP-007-1 R3 (SERC201000675)

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 was in violation of CIP-007-1 R3. Specifically, URE did not adequately test and apply cyber security software patches for all Cyber Assets within the ESP. URE was unable to provide any approved and implemented security patch assessment program for approximately a year and four months from when the Standard became mandatory and enforceable on URE. This original cyber security testing program was not fully implemented because the test environment was unsuitable for the proper testing of cyber security patches due to delays in reaching an operational status for the virtualized test server. URE attested that it was assessing security patches for software on its EMS devices, but did not maintain records of these assessments for all Cyber Assets. URE did not assess patches for other devices within the ESP, because they were end-of-life with no patches to review. As URE assessed patches, if URE determined they were applicable, URE retained the patches for later deployment. Additionally, URE did not deploy security patches until 28 months after the Standard became mandatory and enforceable, when URE began being able to test the security patches.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE established a security patch management process that could be implemented and deployed previously assessed security patches to its identified Cyber Assets.

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. UREs failure to evaluate, test, and deploy security patches left known vulnerabilities on CCAs, Cyber Assets within the ESP, physical access control and monitoring devices, and EACM devices available for exploitation by malicious individuals for a period of over two years. The risk to the reliability of the BPS was mitigated by the following factors. All Cyber Assets were within an ESP and a PSP.

CIP-007-1 R5 (SERC201000676)

CIP-007-1 R5 provides:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> > R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
> >
> > > R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
> > >
> > > R5.1.2. The Responsible Entity shall establish methods, processes, and procedures that generate logs of sufficient detail to create historical audit trails of individual user account access activity for a minimum of ninety days.
> > >
> > > R5.1.3. The Responsible Entity shall review, at least annually, user accounts to verify access privileges are in accordance with Standard CIP-003 Requirement R5 and Standard CIP-004 Requirement R4.
> >
> > R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.
> >
> > > R5.2.1. The policy shall include the removal, disabling, or renaming of such accounts where possible. For such accounts that must remain

enabled, passwords shall be changed prior to putting any system into service.

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

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

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

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

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

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

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-007-1 R5. Specifically, URE did not adequately 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. URE was unable to provide any approved and implemented technical or procedural controls that would enforce authentication for and accountability for shared account usage on any of its Cyber Assets within the ESP prior to approximately two years and three months from when the Standard became mandatory and enforceable on URE. URE acknowledged that no evidence could be provided to demonstrate that logs for the usage of the shared accounts were maintained.

During the assessment conducted by URE into the scope of this violation, it discovered that it maintained several system accounts on its lists, but found additional system accounts it was not

tracking. URE could not provide any evidence that any of these accounts were approved or that access privileges were reviewed annually. These accounts were on EMS devices, CCAs, physical access control system devices, and EACM devices.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE implemented technical or procedural controls to enforce access authentication of, and accountability for, all user activity.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to establish, document, and implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity for shared accounts could allow unauthorized individuals to create new shared accounts or use existing shared accounts to gain access to or control of CCAs, potentially leading to the loss of control or visibility over URE's portion of the BPS. URE did not have documented controls for over two years from the date of compliance. Several URE employees and vendors knew the passwords for shared accounts. The risk to the reliability of the BPS was mitigated by the following factors. URE changed default account passwords, where technically feasible. In addition, all Cyber Assets were within an ESP and a PSP.

CIP-007-1 R5; R5.2.3 and R5.3 (SERC2012010859)
CIP-007-1 R3 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SERC determined that URE was in violation of CIP-007-1 R5.2.3 and R5.3.3. Specifically, URE failed to limit access to shared accounts and failed to document compensating measures for its inability to support password requirements. URE maintained information required for the authentication of approved remote vendor access for support and maintenance in plain sight within the PSP. URE posted a document that provided remote access instructions for a shared account and included the username, password, and a personal identification number on the wall inside the PSP. In addition, a two-factor authentication token required to gain access to the shared account was also posted to the same wall. As a result, anyone inside the PSP would have access to this information. URE thus could not ensure that this information was secured and available only on a need-to-know and as-required basis to authorized individuals. SERC determined that information necessary to gain remote electronic access the ESP was available and accessible to personnel who may not be authorized for remote electronic access, and could be obtained and used to gain unauthorized cyber access to CCAs without the knowledge of and outside of the control of the intended process, in violation of CIP-007 R5.2.3.

In addition, URE also maintained a process support document that specified the minimal password requirements for all types of Cyber Assets included in its CIP program. The process support document did not provide URE guidance on what should occur if a password cannot be established on a Cyber Asset, or if the specific password requirements as specified in CIP-007-1 R5.3 cannot be achieved due to technical limitations. Specifically, in the case of a few global positioning system (GPS) clocks identified during the audit, URE failed to apply its internal password criteria because the GPS clocks could not be logged into and are programmed by the front panel push buttons. URE did not document this fact by requesting a TFE for the GPS clocks, in violation of CIP-007 R5.3.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE through when URE submitted a request for a TFE for password applicability on the GPS clocks.

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 decision to maintain the information required to log remotely into a shared account in an open space could permit visitors or individuals within the PSP to obtain the ability to log into the shared account and have access to CCAs, potentially disrupting URE's control or visibility over its portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. The IP address needed to gain access to the shared account was not posted on the document in the PSP. URE policies required all individuals with authorized access to the PSP to have valid PRAs and required all visitors to be escorted while inside the PSP. The GPS clocks could not be logged into and could only be programmed by physically accessing the devices, which were located within a PSP.

CIP-007-3a R5; R5.3.3 (SERC2011007657)

The purpose statement of Reliability Standard CIP-007-3a provides: "Standard CIP-007-3 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-007-3a 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.

***

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

***

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

CIP-007-3a R5.3 has a "Medium" VRF and a "Severe" VSL.

URE submitted a Self-Report to SERC stating that it was in violation of CIP-007-3a R5.3.3. Specifically, URE failed to change passwords for shared accounts on several Cyber Assets at least annually, as required.

URE had a shared account procedure addressing the set-up, management, and tracking of shared account usage. URE discovered during an internal program assessment that it did not annually change the shared account passwords on several Cyber Assets for the previous year. After making this discovery, URE immediately changed all the affected shared account passwords.

This violation occurred because URE had inadequate alerts and notifications in place to remind administrators to change the passwords for the shared accounts annually. URE previously depended on the annual reviews of access and shared accounts to prompt the administrators to change the passwords for the shared accounts. However, URE's annual review process lacked specific direction and guidance, resulting in URE's failure to change some passwords for some Cyber Assets for the affected year.

SERC determined the duration of the violation to be from the day after URE failed to change the passwords for the shared accounts for the affected year, through when URE changed the missed shared 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 change the shared account passwords annually could give unauthorized individuals more time to guess or otherwise obtain existing passwords on Cyber Assets. This violation affected 43.2% of total Cyber Assets in the URE's CIP program. The risk to the reliability of the BPS was mitigated by the following factors. URE had an

established program for shared accounts that included tracking and assigning access based on roles. All affected Cyber Assets were secured within established ESPs and PSPs which restricted access.

CIP-007-1 R6; R6.3 (SERC2012010858)

CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> ***
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.

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

During the Compliance Audit, SERC determined that URE was in violation of CIP-007-1 R6.3. Specifically, URE failed to maintain logs of system events related to cyber security for all Cyber Assets within the ESP. After the Compliance Audit, URE undertook an internal review and found that besides the GPS clocks and serial communication switches identified by the SERC audit team, several keyboard/video/mouse (KVM) switches, single port serial servers, and network isolation switches were also unable to log system events related to cyber security.

Although URE was aware of these Cyber Assets, it did not believe that it was required to log and maintain logs related to cyber security events because the affected Cyber Assets could not be logged into. As a result, URE did not request a TFE for its inability to log on these Cyber Assets.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE submitted a TFE request for the Cyber Assets that were not capable of logging system events related to cyber security.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although the affected Cyber Assets were incapable of logging, the Cyber Assets connected to them had logging enabled. The affected Cyber Assets were protected within established ESPs and PSPs.

CIP-008-1 R1 (SERC200900420)

The purpose statement of Reliability Standard CIP-008-1 provides: "Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-008-1 R1 provides:

> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:
>
> > R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
> >
> > R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
> >
> > R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.
> >
> > R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.
> >
> > R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
> >
> > R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

CIP-008-1 R1 has a "Lower" VRF and a "Severe" VSL.

During the Spot Check, SERC determined that URE was in violation of CIP-008-1 R1.4. Specifically, URE failed to produce evidence that historical versions of the entity's Cyber Security Incident response plan

contained a process for updating the Cyber Security Incident response plan within 90 calendar days of any changes. URE's Cyber Security Incident response plan failed to include a process to update its Cyber Security Incident response plan within 90 days of any changes. Instead of including a process, URE had a note stating that the response plan should be updated with 90 days of any changes and specified the individual who would conduct the updates. However, the response plan did not provide guidance or instructions about how updates would be made. URE's Cyber Security Incident response plan did not include a process for updating the response plan within 90 days until it was revised.

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 Cyber Security Incident response plan to include a process for updating the response plan within 90 days of a change.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE's response plan did not include a process for updating the response plan within 90 days of any change, the response plan noted that it should be updated within 90 days of any change. URE also documented an update to the response plan several months before documenting a process for updating the response plan.

CIP-009-1 R1 SERC201000677

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

CIP-009-1 R1 provides:

> R1. Recovery Plans — The Responsible Entity shall create and annually review recovery plan(s) for Critical Cyber Assets. The recovery plan(s) shall address at a minimum the following:
>
> > R1.1. Specify the required actions in response to events or conditions of varying duration and severity that would activate the recovery plan(s).
> >
> > R1.2. Define the roles and responsibilities of responders.

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

URE submitted a Self-Report to SERC stating that it was in violation of CIP-009-1 R4. Specifically, URE did not have sufficient processes and procedures for the backup and storage of information required to restore CCAs. SERC later determined that URE did not have a recovery plan for CCAs for approximately two years, and decided to address the violation under CIP-009-1 R1.

URE had a high-level business continuity plan that addressed the loss and recovery of systems and sites like the EMS or control centers, but did not provide granular detail on how to recover CCAs. URE's business continuity plans also addressed at a high level the backup and storage of information necessary to restore the EMS or control centers. URE later approved a recovery plan for CCAs.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when URE implemented a documented recovery plan for 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. URE's failure to create a recovery plan for CCAs could delay the recovery of CCAs in the event that CCAs became non-functional, which could affect URE's visibility of or control over its portion of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. URE had high-level business continuity plans that could be used to assist in the recovery of CCAs. These business continuity plans also addressed how URE should backup and store information necessary for the recovery of systems, which could be used to assist in the recovery of CCAs. The business continuity plan had procedures to operate in a manual mode while some or all Cyber Assets were in recovery mode. URE also had an experienced SME with the knowledge and experience necessary to recover CCAs from an event.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of fifty thousand dollars ($50,000) 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 the violations of CIP-003-1 R4, R5, and R6; CIP-004-1 R1 and R4; CIP-004-3 R3; CIP-005-1 R1, R2, R3 and R5; CIP-006-3c R1 and R8; CIP-007-1 R2, R3, and R5; and CIP-007-3a R5;
3. URE was cooperative throughout the compliance enforcement process;

4. URE had a compliance program at the time of the violations, which SERC considered a mitigating factor;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations of CIP-007-1 R2 and R3, which posed a serious and substantial risk to the reliability of the BPS , the remainder of the violations did not pose a serious or substantial risk to the reliability of the BPS , as discussed above;
7. URE has committed to performing certain above and beyond activities, which SERC considered a mitigating factor in the penalty;[4].
8. URE expended additional effort to set up its original CIP program and committed to further enhancements to the program; and
9. 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 fifty thousand dollars ($50,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[5]

CIP-002-1 R3 (SERC200900414)
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to SERC on. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003349-1 and was submitted as non-public information to FERC in accordance with FERC orders.

[4] URE has committed to conducting a review of its current procedures regarding compliance with NERC CIP Standards. This review will address the sustainability of the procedures and associated processes through the remaining tenure of the current version of the CIP Standards, but will focus primarily on the needed changes to ensure that these procedures and processes are sustainable as URE transitions to Version 5 of the CIP Standards. As part of this review, URE will prepare and deliver a report to SERC that will detail URE's findings as part of its review and actions plans to address any areas of concern. URE will provide SERC with high-level status updates on the progress of its review of its CIP procedures. In addition, URE has agreed to have SERC conduct a Spot Check of its CIP compliance program, which will focus on URE's adherence to the procedures in place, progress on implementing any action plans identified in its report, and validating completion of the mitigation plans submitted to remediate the violations identified in this settlement agreement.
[5] *See* 18 C.F.R § 39.7(d)(7). SERC requested revisions of several Mitigation Plans but did not reject any of the Mitigation Plans. The Mitigation Plans addressed in this document are the most recent approved versions.

URE's Mitigation Plan required URE to:

1. disable the ability of the EMS console to initiate supervisory controls to bulk electric system assets;
2. add network switches to the CCA list;
3. establish a new policy governing the identification of CCAs and non-critical Cyber Assets; and
4. train employees on the new policy and its associated processes.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-003-1 R1; R1.2 (SERC200900415)

URE's Mitigation Plan to address its violation of CIP-003-1 R1.2 was submitted to SERC on. The Mitigation Plan was accepted by SERC and approved by NERC . The Mitigation Plan for this violation is designated as SERCMIT003350-1 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. send the URE cyber security policy to the EMS vendor; and
2. implement a policy in which future lists of authorized vendor employees contained a confirmation that the personnel had been provided copies of the URE cyber security policy.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-003-1 R4 (SERC201000665)

URE's Mitigation Plan to address its violation of CIP-003-1 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005807-1 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a new program for information protection with a policy, plans, procedures, records, and meaningful definitions;

2. mark the new documents as protected under the new information protection program where appropriate; and
3. provide training to employees on the new CIP program, including information protection

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-003-1 R5 (SERC201000666)

URE's Mitigation Plan to address its violation of CIP-003-1 R5 was submitted to stating it had been completed on. The Mitigation Plan was accepted by SERC on and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005808-1 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a new information protection program that includes multiple classification levels and uses the same processes and forms for granting and managing information protection access as for physical and electronic access to simplify and eliminate unnecessary documentation; and
2. provide training on the new program to employees that use protected information.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-003-1 R6 (SERC201000667)

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010115 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop an interim change control process that could be manually maintained;
2. review and update the entire CIP program;
3. implement a new change control and configuration management policy, process, and other documents; and
4. provide training to relevant personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-003-3 R6 (SERC2012010852)

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008083-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update its training material to include more detail about the change control process and emphasized the need to closely follow the process; and
2. train affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-1 R1 (SERC201000507)

URE's Mitigation Plan to address its violation of CIP-004-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003384 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to send a cyber security awareness reminder email to the vendor employees.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-1 R2; R2.1 (SERC200900416)

URE's Mitigation Plan to address its violation of CIP-004-1 R2.1 and R2.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003351-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. train all personnel who had not been previously trained;
2. receive a list of EMS vendor employees who need access confirming that they had completed URE training;
3. document that all personnel with access had completed the training;
4. implement steps to improve the processes and documentation of training by requiring EMS vendor employees to individually sign and date the training form as evidence of completion;
5. implement a new process to ensure that necessary PRAs and training were completed before access was granted and renewed as required. The employee responsible for granting and reviewing access was involved in developing the process so specific training was not needed; and
6. train other employees about the access request process as part of the new CIP program roll-out.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-1 R3 (SERC200900417)

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to SERC . The Mitigation Plan was accepted by SERC and approved by NERC . The Mitigation Plan for this violation is designated as SERCMIT003352-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete PRAs for all personnel who still had access and who did not have a PRA on file;
2. review and significantly update its CIP policies, processes, and procedures, which now include a new access request process that ensures PRAs are current before access is granted; and
3. develop a spreadsheet which it uses to track when PRAs were last completed and due for renewal.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-3 R3; R3.2 (SERC2011007656)

URE's Mitigation Plan to address its violation of CIP-004-3 R3.2 was submitted to SERC stating it had been completed. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005538 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke access by the affected employees to CCAs;
2. initiate new PRA updates;
3. set up structured calendar events for all responsible personnel, highlighting all deadlines initiated by the new CIP process;
4. establish monthly meetings to review CIP-related tasks that have to be performed; and
5. assign an employee to make sure regularly scheduled CIP-related tasks are being completed on time

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-1 R4 (SERC200900419)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC . The Mitigation Plan for this violation is designated as SERCMIT003353-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. revoke PSP access for the emergency access card;
2. initiate a project to thoroughly review and update its entire CIP management program, including access control;
3. work with an expert consultant to develop new policies, processes, procedures, and other documents; and
4. use the new processes to identify and record the details of the specific electronic and physical access rights of individuals; and
5. finalize the new CCA access lists.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-004-1 R4 (SERC201000668)

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005809 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a role-based access program for both physical and electronic access; and
2. list all individuals with any type of access along with the roles they are permitted to perform and the date the roles were granted.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R1; R1.1 and R1.4 (SERC201000669)

URE's Mitigation Plan to address its violation of CIP-005-1 R1.1 and R1.4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005810-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. update the list of Cyber Assets to include the SONET nodes and the terminal servers;
2. implement a new process to identify CCAs and non-critical Cyber Assets that begins with a full inventory of all Cyber Assets located inside PSPs and ESPs;
3. develop a new process to establish ESPs and access points for the CCAs; and
4. provide training to affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R1; R1.5 (SERC201000670)

URE's Mitigation Plan to address its violation of CIP-005-1 R1.5 was submitted to SERC. The Mitigation Plan was accepted by SERC on and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005811-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a two-factor authentication solution for remote access. All remote access control and monitoring is now handled by the ESP access point in conjunction with the two-factor authentication solution, eliminating this role from the VPN termination point;
2. revise its ESP drawing to show the front-end processors on the ESP border, properly documenting them as access points;
3. change the default account passwords;
4. set up structured calendar events for all responsible personnel that highlight all deadlines initiated by the new CIP process;
5. establish monthly meetings to review CIP-related tasks that have to be performed; and
6. assign an employee to make sure that regularly scheduled CIP-related tasks are completed on time.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R1; R1.5 (SERC2012010853)

URE's Mitigation Plan to address its violation of CIP-005-1 R1.5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008084-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. enhance the written testing procedures to include the use of detailed test scripts and a requirement to retain these scripts and results of testing as part of the change control process;
2. update its training to reflect the test procedure changes, including more detail about the change control process and emphasize the need to follow the process closely; and

3. provide training to appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R2; R2.2 (SERC201000671)
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 is designated as SERCMIT005812-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop and implement a new change control process;
2. develop and implement a process to develop baseline profiles to document control of electronic access at the ESP access point firewalls;
3. train all employees who use the processes; and
4. close all ports that were identified as not needed.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-3a R2; R2.2 (SERC2012010854)
URE's Mitigation Plan to address its violation of CIP-005-3a R2.2 was submitted to SERC . The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008085-1 and was submitted as non-public information to FERC in accordance with FERC orders.
URE's Mitigation Plan required URE to:

1. conduct a thorough review of the firewall open ports and note any ports that were not necessary or that could be opened to a smaller group of assets;
2. request additional information from the vendor regarding open port requirements;
3. develop an action plan to close unneeded ports and limit needed ports only to those assets that needed to use them; and
4. carry out the action plan under the change control process.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R2; R2.5.2 (SERC200900418)

URE's Mitigation Plan to address its violation of CIP-005-3a R2.2 was submitted to SERC on. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT010102 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to submit a TFE that included documentation of the mitigating strong controls being used.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R3 (SERC201000672)

URE's Mitigation Plan to address its violation of CIP-005-1 R3 was submitted to SERC on. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005813-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop new processes for monitoring and logging; and
2. develop profiles to document the setup of monitoring and logging of electronic access at the ESP access point firewalls

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R3; R3.2 (SERC2012010857)

URE's Mitigation Plan to address its violation of CIP-005-1 R3.2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008086-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. submit TFEs for the affected devices;
2. update its training materials to include more detail about the change control process, including the need for the asset owner to review the change and determine if any TFEs are required; and
3. provide training to affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-005-1 R5; R5.1 (SERC201000673)

URE's Mitigation Plan to address its violation of CIP-005-1 R5.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005817-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. conduct a thorough review of its entire CIP program and develop a new suite of CIP policies and associated documents that could be managed without the need for a sophisticated software tool. The new documents developed included replacements for the functionality outlined in those documents that missed the annual review;
2. set up structured calendar events for all responsible personnel, highlighting all deadlines initiated by the new CIP process;
3. establish monthly meetings to review CIP-related tasks that have to be performed; and
4. assign an employee to make sure regularly scheduled CIP-related tasks are being completed on time.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-006-3c R1; R1.6 (SERC2013012192)

URE's Mitigation Plan to address its violation of CIP-006-3c R1.6 was submitted to SERC on. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT009160 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. eliminate the use of the PCC and BCC for non-business related group gatherings;
2. notify all personnel with authorized PSP access of this change in policy and remind them of their responsibilities within the PSP;
3. develop a training program specifically for PSP access that all personnel with authorized PSP access will be required to take and test on.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-006-1 R1; R1.8 (SERC2012010637)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT007646 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove write permissions from the PCC and BCC partition and remove network access from the server, thus disabling the ability to change the access control devices for the PSP; and
2. purchase and install a stand-alone access control, monitoring, and alarming system for the PCC and BCC.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-006-1 R1; R1.8 (SERC2012010855)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to SERC . The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008087-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. enhance the written testing procedures to include the use of detailed test scripts and a requirement to retain the test scripts and results of testing as part of the change control process;
2. update its training material to reflect the test procedure changes, including more detail about the change control process and emphasize the need to follow the process closely; and
3. provide training to affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-006-3c R8; R8.1 (SERC20120009690)

URE's Mitigation Plan to address its violation of CIP-006-3c R8.1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT006728-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change the testing cycle time from the minimum three years in the CIP Standard to an annual testing cycle;
2. set up structured calendar events for all responsible personnel, highlighting all deadlines initiated by the new CIP process;
3. establish monthly meetings to review CIP-related tasks that have to be performed;
4. assign an employee to make sure regularly scheduled CIP-related tasks are being completed on time;
5. hold a meeting with the person responsible for testing and other stakeholders to make sure the annual testing cycle was understood; and
6. test the PACM devices.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R1; R1.3 (SERC2012010856)

URE's Mitigation Plan to address its violation of CIP-007-1 R1.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008088-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. enhance the written testing procedures to include the use of detailed test scripts and a requirement to retain the test scripts and results of testing as part of the change control process;
2. update its training to reflect the test procedure changes; and
3. provide training to affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R2 (SERC201000674)

URE's Mitigation Plan to address its violation of CIP-007-1 R12 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005814-3 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. replace its former EMS with a modern solution and require the vendor to provide the information necessary to build baseline profiles completely and accurately;
2. develop and implement a new change control process;
3. develop and implement processes to build baseline profiles;
4. provide training to employees who used the new processes; and
5. develop baseline profiles for the new EMS to document the ports and services used by the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R3 (SERC201000675)

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005815-2 and was submitted as non-public information to in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. implement a virtual server and network to test security patches before applying;
2. test workstations by creating a clone image of a workstation and put it on another off-line workstation;
3. perform analyses after patches were applied in the test environment to see if the patch opened any additional ports, added services, or added users;
4. conduct a thorough review of its entire CIP program;
5. develop a new test plan and procedure; and
6. provide training to affected personnel on the changes.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R5 (SERC201000676)

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005816-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a new program for access control and account management with associated policies, plans, procedures, and records;
2. train personnel on the new program; and
3. create a database application to log shared account usage by allowing the support staff to create log entries by pre-populating known information and more easily populate other fields with a mouse click.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R5; R5.2.3 and R5.3 (SERC2012010859)

URE's Mitigation Plan to address its violation of CIP-007-1 R5.2.3 and R5.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT008089-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. move the two-factor authentication token to a private location and kept it separate from the username and password information;
2. revoke the EMS vendor access at the end of the availability test; and
3. submit a TFE for the GPS clocks.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-3a R5; R5.3.3 (SERC2011007657)

URE's Mitigation Plan to address its violation of CIP-007-3a R5.3.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005609 and was submitted as non-public information to FERC on in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. change and document the shared account passwords using URE's new CIP process;
2. set up structured calendar events for all responsible personnel, highlighting all deadlines initiated by the new CIP process;
3. establish monthly meetings to review CIP-related tasks that have to be performed;
4. assign an employee to make sure regularly scheduled CIP-related tasks are being completed on time.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-007-1 R6; R6.3 (SERC2012010858)

URE's Mitigation Plan to address its violation of CIP-007-1 R6.3 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC . The Mitigation Plan for this violation is designated as SERCMIT008090-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. submit TFEs for the affected devices;
2. update its training materials to include more detail about the change control process, including the need for the asset owner to review the change and determine if any TFEs are required; and
3. provide training to affected personnel.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-008-1 R1 (SERC200900420)

URE's Mitigation Plan to address its violation of CIP-008-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003354-1 and was submitted as non-public information to FERC on December 9, 2013 in accordance with FERC orders.

URE's Mitigation Plan required URE to revise its Cyber Security Incident response plan to specify that the plan must be updated with any changes made within 90 days of the change.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

CIP-009-1 R1 (SERC201000677)

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT005818-2 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. work with an experienced consultant to develop a comprehensive recovery plan that addresses specific types of CCAs and includes processes and procedures for backup and storage of information required to restore CCAs; and
2. train personnel on the new plan.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SERC.

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 fifty thousand dollar ($50,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. the violations constituted URE's first occurrence of violations of the subject NERC Reliability Standards;
2. URE self-reported the violations, as discussed 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;

[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).

5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. SERC determined that the violations of CIP-007-1 R2 and R3 posed a serious and substantial risk to the reliability of the BPS; however, the remainder of the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. URE has committed to performing certain above and beyond activities, which SERC considered a mitigating factor in the penalty determination, as discussed above;
8. URE expended additional effort to set up its original CIP program and committed to further enhancements to the program; and
9. 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 fifty thousand dollars ($50,000) 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.

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

In accordance with the Commission's Rules of Practice and Procedure, 18 C.F.R. § 388.112, a non-public version of the information redacted from the public filing is being provided under separate cover.

Because certain of the attached documents are deemed confidential by NERC, Registered Entities and Regional Entities, NERC requests that the confidential, non-public information be provided special treatment in accordance with the above regulation.

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between SERC and URE, included as Attachment a;

b) Record documents for the violation of CIP-002-1 R3 (SERC200900414), included as Attachment b:

   1. URE's Source Document ;
   2. URE's Mitigation Plan designated as SERCMIT003349-1 ;
   3. URE's Certification of Mitigation Plan Completion;

c) Record documents for the violation of CIP-003-1 R1; R1.2 (SERC200900415), included as Attachment c:

   1. URE's Source Document;
   2. URE's Mitigation Plan designated as SERCMIT003350-1;
   3. URE's Certification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-003-1 R4 (SERC201000665), included as Attachment d:

   1. URE's Self-Report ;
   2. URE's Mitigation Plan designated as SERCMIT005807-1;
   3. URE's Certification of Mitigation Plan Completion;

e) Record documents for the violation of CIP-003-1 R5 (SERC201000666), included as Attachment e:

   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT005808-1;
   3. URE's Certification of Mitigation Plan Completion;

f) Record documents for the violation of CIP-003-1 R6 (SERC201000667), included as Attachment f:

   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as SERCMIT010115;
   3. URE's Certification of Mitigation Plan Completion;

g) Record documents for the violation of CIP-003-3 R6 (SERC2012010852), included as Attachment g:

   1. URE's Source Document;

2. URE's Mitigation Plan designated as SERCMIT008083-1;
3. URE's Certification of Mitigation Plan Completion;

h) Record documents for the violation of CIP-004-1 R1 (SERC201000507), included as Attachment h:
1. URE's Self-Report dated;
2. URE's Mitigation Plan designated as SERCMIT003384;
3. URE's Certification of Mitigation Plan Completion;

i) Record documents for the violation of CIP-004-1 R2; R2.1 (SERC200900416), included as Attachment i:
1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT003351-1;
3. URE's Certification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-004-1 R3 (SERC200900417), included as Attachment j:
1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT003352-1;
3. URE's Certification of Mitigation Plan Completion;

k) Record documents for the violation of CIP-004-3 R3; R3.2 (SERC2011007656), included as Attachment k:
1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005538;
3. URE's Certification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-004-1 R4 (SERC200900419), included as Attachment l:
1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT003353-1;
3. URE's Certification of Mitigation Plan Completion;

m) Record documents for the violation of CIP-004-1 R4 (SERC201000668), included as Attachment m:
1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005809;

3. URE's Certification of Mitigation Plan Completion;

n) Record documents for the violation of CIP-005-1 R1; R1.1; R1.4 (SERC201000669), included as Attachment n:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005810-1;
3. URE's Certification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-005-1 R1; R1.5 (SERC201000670), included as Attachment o:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005811-1;
3. URE's Certification of Mitigation Plan Completion;

p) Record documents for the violation of for CIP-005-1 R1; R1.5 (SERC2012010853), included as Attachment p:

1. URE's Source Document dated August 6, 2012;
2. URE's Mitigation Plan designated as SERCMIT008084-1;
3. URE's Certification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-005-1 R2; R2.2 (SERC201000671), included as Attachment q:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005812-1;
3. URE's Certification of Mitigation Plan Completion;

r) Record documents for the violation of CIP-005-3a R2; R2.2 (SERC2012010854), included as Attachment r:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008085-1;
3. URE's Certification of Mitigation Plan Completion;

s) Record documents for the violation of CIP-005-1 R2; R2.5.2 (SERC200900418), included as Attachment s:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT010102;
3. URE's Certification of Mitigation Plan Completion;

t) Record documents for the violation of CIP-005-1 R3 (SERC201000672), included as Attachment t:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005813-1;
3. URE's Certification of Mitigation Plan Completion;

u) Record documents for the violation of CIP-005-1 R3; R3.2 (SERC2012010857), included as Attachment u:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008086-2;
3. URE's Certification of Mitigation Plan Completion;

v) Record documents for the violation of CIP-005-1 R5; R5.1 (SERC201000673), included as Attachment v:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005817-1;
3. URE's Certification of Mitigation Plan Completion;

w) Record documents for the violation of CIP-006-3c R1; R1.6 (SERC2013012192), included as Attachment w:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT009160;
3. URE's Certification of Mitigation Plan Completion;

x) Record documents for the violation of CIP-006-1 R1; R1.8 (SERC2012010637), included as Attachment x:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT007646;
3. URE's Certification of Mitigation Plan Completion;

y) Record documents for the violation of CIP-006-1 R1; R1.8 (SERC2012010855), included as Attachment y:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008087-1;
3. URE's Certification of Mitigation Plan Completion;

z) Record documents for the violation of for CIP-006-3c R8; R8.1 (SERC2012009690), included as Attachment z:

1. URE's Self-Report date;
2. URE's Mitigation Plan designated as SERCMIT006728-1;
3. URE's Certification of Mitigation Plan Completion;

aa) Record documents for the violation of CIP-007-1 R1; R1.3 (SERC2012010856), included as Attachment aa:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008088-1;
3. URE's Certification of Mitigation Plan Completion;

bb) Record documents for the violation of CIP-007-1 R2 (SERC201000674), included as Attachment bb:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005814-3;
3. URE's Certification of Mitigation Plan Completion;

cc) Record documents for the violation of CIP-007-1 R3 (SERC201000675), included as Attachment cc:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005815-2;
3. URE's Certification of Mitigation Plan Completion;

dd) Record documents for the violation of CIP-007-1 R5 (SERC201000676), included as Attachment dd:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005816-1;
3. URE's Certification of Mitigation Plan Completion;

ee) Record documents for the violation of CIP-007-1 R5; R5.2.3; R5.3 (SERC2012010859), included as Attachment ee:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008089-1;
3. URE's Certification of Mitigation Plan Completion;

ff) Record documents for the violation of CIP-007-3a R5; R5.3.3 (SERC2011007657), included as Attachment ff:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005609;
3. URE's Certification of Mitigation Plan Completion;

gg) Record documents for the violation of CIP-007-1 R6; R6.3 (SERC2012010858), included as Attachment gg:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT008090-2;
3. URE's Certification of Mitigation Plan Completion;

hh) Record documents for the violation of CIP-008-1 R1 (SERC200900420), included as Attachment hh:

1. URE's Source Document;
2. URE's Mitigation Plan designated as SERCMIT003354-1;
3. URE's Certification of Mitigation Plan Completion;

ii) Record documents for the violation of CIP-009-1 R1 (SERC201000677), included as Attachment ii:

1. URE's Self-Report;
2. URE's Mitigation Plan designated as SERCMIT005818-2; and
3. URE's Certification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net John R. Twitchell* VP and Chief Program Officer SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8205 (704) 357-7914 – facsimile jtwitchell@serc1.org Andrea B. Koch* Director of Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8219 (704) 357-7914 – facsimile akoch@serc1.org	Sonia C. Mendonça* 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 James M. McGrane* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 494-7787 (704) 357-7914 – facsimile msifontes@serc1.org jmcgrane@serc1.org

*Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.	

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments