PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

July 31, 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 1 and Unidentified Registered Entity 2,
FERC Docket No. NP13-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE1), NERC Registry ID# NCRXXXXX, and Unidentified Registered Entity 2 (URE2), NERC Registry ID# NCRXXXXX, collectively (URE), 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 Reliability*First*, SERC (collectively, the Regions), and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from Reliability*First* and SERC's determination and findings of the violations[3] of CIP-002-3, CIP-003-3, CIP-004-3, CIP-005-3, CIP-005-3a, CIP-006-3, CIP-006-3c, CIP-007-3, CIP-007-3a, CIP-008-3, and CIP-009-3. According to the Settlement Agreement, URE admits to the violations. URE1 and URE2 have each

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2011). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged or confirmed violation. These violations span versions 1 through 3 of the Standard. For ease of reference, version 3 will be used throughout this document. This is not applicable in instances where other versions are referenced.

agreed to the assessed penalty of one hundred seventy-five thousand dollars ($175,000), for a total penalty of three hundred fifty thousand dollars ($350,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification Numbers RFC2011001057, RFC2011001243, RFC2012001319, SERC2011008000, SERC2011007525, RFC2011001058, SERC2011007658, RFC2012010396, SERC2013011704, RFC2012009880, SERC2013011710, SERC2011008269, RFC2011001244, RFC2011001264, SERC2013011705, RFC201100876, RFC2012001318, SERC2011007571, RFC2012001317, SERC2011008270, RFC2012001316, RFC201100877, SERC2011007871, RFC2012010397, RFC201100878, SERC2013011711, SERC2013011771, SERC2011007872, SERC2011008001, SERC2011007881, RFC201100879, RFC201100880, RFC2013011723, RFC2012009881, RFC2012001315, RFC2011001112, SERC2011007998, RFC2011001060, SERC2011007574, RFC201100881, RFC2011001062, RFC2011001113, RFC2012001314, SERC2011007981, SERC2011007570, SERC2011007573, RFC201100882, RFC2011001064, RFC2011001114, SERC2011007880, SERC2011007572, SERC2011008002, SERC2011008272, RFC201100883, RFC2011001245, SERC2011007870, RFC2012010398, SERC2013011712, RFC2012010400, and SERC2013011709 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 May 21, 2013, by and between Reliability*First*, 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
ReliabilityFirst Corporation and SERC Reliability Corporation	Unidentified Registered Entity 1 and Unidentified Registered Entity 2	NOC-1998	RFC2011001057	CIP-002-3	R3	High	$350,000
			RFC2011001243	CIP-002-3	R3	High	
			RFC2012001319	CIP-002-3	R3	High	
			SERC2011008000	CIP-002-3	R3	High	
			SERC2011007525	CIP-002-3	R3	High	
			RFC2011001058	CIP-003-3	R4	Medium	
			SERC2011007658	CIP-003-3	R4	Medium	
			RFC2012010396	CIP-003-3	R5	Lower	
			SERC2013011704	CIP-003-3	R5	Lower	
			RFC2012009880	CIP-003-3	R6	Lower	
			SERC2013011710	CIP-003-3	R6	Lower	
			SERC2011008269	CIP-003-3	R6	Lower	
			RFC2011001244	CIP-004-3	R4	Lower	
			RFC2011001264	CIP-004-3	R4	Lower	
			SERC2013011705	CIP-004-3	R4	Lower	
			SERC201000506	CIP-004-3	R4	Lower	
			RFC201100876	CIP-005-3	R1	Medium	
			RFC2012001318	CIP-005-3	R1	Medium	

ReliabilityFirst Corporation and SERC Reliability Corporation	Unidentified Registered Entity 1 and Unidentified Registered Entity 2	NOC-1998	SERC2011007571	CIP-005-3	R1	Medium	$350,000
			RFC2012001317	CIP-005-3	R2	Medium	
			SERC2011008270	CIP-005-3	R2	Medium	
			RFC2012001316	CIP-005-3a	R3	Medium	
			RFC201100877	CIP-005-3a	R4	Medium	
			SERC2011007871	CIP-005-3a	R4	Medium	
			RFC2012010397	CIP-005-3	R5	Lower	
			RFC201100878	CIP-006-3	R1	Medium	
			SERC2013011711	CIP-006-3	R1	Medium	
			SERC2013011771	CIP-006-3	R1	Medium	
			SERC2011007872	CIP-006-3	R1	Medium	
			SERC2011008001	CIP-006-3	R1	Medium	
			RFC201100879	CIP-006-3	R2	Medium	
			SERC2011007881	CIP-006-3	R2	Medium	
			RFC201100880	CIP-006-3	R4	Medium	
			RFC2012010022	CIP-006-3c	R5	Medium	
			RFC2013011723	CIP-006-3c	R5	Medium	
			RFC2012009881	CIP-007-3	R1	Medium	
			RFC2012001315	CIP-007-3	R2	Medium	

ReliabilityFirst Corporation and SERC Reliability Corporation	Unidentified Registered Entity 1 and Unidentified Registered Entity 2	NOC-1998	RFC2011001112	CIP-007-3	R3	Lower	$350,000
			SERC2011007998	CIP-007-3	R3	Lower	
			RFC2011001060	CIP-007-3	R4	Medium	
			SERC2011007574	CIP-007-3	R4	Medium	
			RFC201100881	CIP-007-3	R5	Lower	
			RFC2011001062	CIP-007-3	R5	Lower	
			RFC2011001113	CIP-007-3	R5	Lower	
			RFC2012001314	CIP-007-3	R5	Lower	
			SERC2011007981	CIP-007-3	R5	Lower	
			SERC2011007570	CIP-007-3	R5	Lower	
			SERC2011007573	CIP-007-3	R5	Lower	
			RFC201100882	CIP-007-3	R6	Lower	
			RFC2011001064	CIP-007-3	R6	Lower	
			RFC2011001114	CIP-007-3	R6	Lower	
			SERC2011007880	CIP-007-3	R6	Lower	
			SERC2011007572	CIP-007-3	R6	Lower	
			SERC2011008002	CIP-007-3	R6	Lower	
			SERC2011008272	CIP-007-3	R6	Lower	
			RFC201100883	CIP-007-3a	R8	Lower	

ReliabilityFirst Corporation and SERC Reliability Corporation	Unidentified Registered Entity 1 and Unidentified Registered Entity 2	NOC-1998	RFC2011001245	CIP-007-3a	R8	Lower	$350,000
			SERC2011007870	CIP-007-3a	R8	Lower	
			RFC2012010398	CIP-008-3	R1	Lower	
			SERC2013011712	CIP-008-3	R1	Lower	
			RFC2012010400	CIP-009-3	R5	Lower	
			SERC2013011709	CIP-009-3	R5	Lower	

CIP-002-3

The purpose statement of Reliability Standard CIP-002-3 provides:

> NERC Standards CIP-002-3 through CIP-009-3 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed.
>
> Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.
>
> Standard CIP-002-3 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-002-3 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 inter-utility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002-3, 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-002-3 R3 has a "High" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE2 self-reported a violation of CIP-002-3 R3 to SERC. URE2 discovered that, due to a clerical error, it failed to include 44 devices on its initial Critical Cyber Asset (CCA) list signed by the senior executive. URE2 provided the requisite protections to the CCAs at all times, except where URE had a violation described herein.

URE self-reported additional violations of CIP-002-3 R3 to Reliability*First* and SERC. URE uses an asset database for tracking CCAs, which is an automated CCA identification method. However, the asset discovery mechanism in the asset database only properly identified those assets that have the asset client installed, which can only be installed on certain operating systems. As a result, the asset database omitted 58 URE1 devices and 53 URE2 devices that run operating systems that do not support the asset client. Of the 58 URE1 devices, 46 are CCAs. Of the 53 URE2 devices, 34 are CCAs.

URE2 self-reported an additional violation of CIP-002-3 R3 to SERC. In the fall of 2010, technicians connected five devices at two URE2 transmission substations when the substations were converted to Internet Protocol, making the devices accessible remotely. URE2 failed to evaluate the five Cyber

Assets at the substations prior to determining whether they were CCAs and prior to connecting them to the Electronic Security Perimeter (ESP). In the summer of 2011, URE2 disconnected four of the devices, and a week later, URE2 disconnected the remaining device.

URE1 submitted two Self-Reports to Reliability*First* identifying an additional violation of CIP-002-3 R3. For one facility, URE1 failed to evaluate three devices as CCAs. These devices were non-critical Cyber Assets within the ESP and URE afforded them the protections of the ESP. In addition, URE1 connected a laptop computer to the controls network in order to resolve an issue during blackstart testing at a facility. URE1 determined that the only way to resolve expeditiously the issue that occurred, which was related to the emissions system, was to utilize this laptop. URE did not evaluate the laptop for the potential to be a CCA, and as a result, the laptop was not identified and protected as a CCA. Although the laptop was essential to the operation of the Critical Asset during that time, it was not routable outside of the ESP and therefore URE would not have classified it as a CCA.

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-002-3 R3. URE1 submitted a Self-Report to Reliability*First* identifying the same violation of CIP-002-3 R3 in Reliability*First.* URE failed to assess the following two types of interfaces to determine whether they were CCAs: 1) the server management interface that communicates within a control center using a routable protocol; and 2) the virtual infrastructure interface that communicates on a private network within a control center using a routable protocol. For two of URE's functions, URE1 failed to assess 128 Cyber Assets, and URE2 failed to assess 166 Cyber Assets. Furthermore, these Cyber Assets were not logically located within ESPs. Upon assessment, URE determined that 30 of these are CCAs and the remaining 264 are non-critical Cyber Assets.

The Regions determined that URE had a violation of CIP-002-3 R3 because it failed to include certain Cyber Assets on its list of CCAs.

The Regions determined the duration of the violation from the first Self-Report to be from the date the Standard became mandatory and enforceable as to URE2 through when a senior executive signed the revised CCA list.

The Regions determined the duration of the violation from the second Self-Reports to be from the date the Standard became mandatory and enforceable as to URE through the date URE appropriately identified all missing Cyber Assets and added them to the CCA list.

The Regions determined the duration of the violation from the third Self-Report to be from the date URE2 connected the devices to the ESP, through the date URE2 removed the last device from the ESP.

The Regions determined the duration of the violation from the fourth Self-Reports related to the three devices to be from the date the affected Critical Asset had CCAs commissioned through when URE included the affected devices in assessment and the CCA list and afforded them the protective measures of the CIP Standards. The duration related to the laptop computer was one day when URE1 connected the laptop to the controls network.

The Regions determined the duration of the violation from SERC's Compliance Audit to be from the effective date of CAN-0005 through the date URE2 added the affected devices to its CCA list.

The Regions determined that this violation posed a serious or substantial risk to the reliability of the bulk power system (BPS). Unidentified CCAs increase the likelihood that an entity will fail to afford Cyber Assets which are essential to the operation of Critical Assets the security protections of CIP-003 through CIP-009. URE failed on numerous occasions to identify CCAs. Regarding the server management interface devices, unauthorized personnel could gain access to these devices and compromise or disable the CCAs residing on the server, resulting in a loss of monitoring or control. An individual could access the remaining devices if there were a physical breach.

The risk to the BPS was mitigated by the following factors. Regarding the 44 devices, at issue from the first Self-Report, that URE2 inadvertently left off of the CCA list due to the spreadsheet filter issue, URE2 provided CCA protections as required by the CIP Standards to the devices for the duration of the violation.

URE1 afforded the protections of CIP-007-3 R6 to the devices at issue in the second Self-Reports. As a result, those devices were logging and being monitored for cybersecurity events and alerting URE of such events. In addition, these devices are secured with complex passwords, they are located in a Physical Security Perimeter (PSP) that is monitored 24 hours a day, seven days a week, and they are located in an ESP that limits any remote access.

Regarding the five devices at two URE2 substations at issue from the third Self-Report, URE has several protections in place that reduce the risk to reliability of the BPS. In addition to site physical security, which includes fencing and a locked gate, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service

group. Only those with authorized unescorted physical access to the devices could gain local access, and only those with personnel risk assessments (PRAs) and cybersecurity training are eligible for such access.

Regarding the three devices deemed to be non-critical Cyber Assets, at issue from the fourth Self-Report, URE has several protections in place that reduce the risk to reliability of the BPS. In addition to site physical security which includes fencing and a locked gate, all devices were located within a PSP. Furthermore, URE protected and fully prohibited remote access to the applicable devices. Only those with authorized unescorted physical access to the devices could gain local access, and only those with PRAs and cybersecurity training are eligible for such access.

Regarding the laptop, also at issue from the fourth Self-Report, connected to the network during blackstart testing, URE1 took certain steps prior to connecting the laptop to the network, including, updating antivirus definitions, performing an antivirus scan, installing available Windows updates, and updating firewall software and other software. In addition, URE1 isolated the network prior to connecting the laptop and only individuals who had cybersecurity training and PRAs logged into the laptop to resolve the issue. Upon evaluation, URE1 determined that although the laptop was essential to the operation of the Critical Assets during that time, it was not routable outside of the ESP and therefore URE would not have classified it as a CCA.

Regarding the devices at issue in the SERC Compliance Audit finding and the fifth Self-Report to Reliability*First*, URE afforded the following protections, where technically feasible: access control, firewalls and routers, intrusion detection, logging, event monitoring, antivirus and malware protection, assessment, demilitarized zone architecture, security patch management, remote access, file transfers, six-wall boundaries, restricted card access, alarm contacts at access points without card access, and security monitoring. When it was technically infeasible to provide the protections, URE submitted TFEs, which were approved. Regarding the virtual infrastructure interface, the likelihood of logical access is decreased since the affected devices do not communicate outside the network.

CIP-003-3

The purpose statement of Reliability Standard CIP-003-3 provides: "Standard CIP-003-3 requires that Responsible Entities[4] have minimum security management controls in place to protect Critical Cyber

[4] Within the text of Standard CIP-002 through CIP-009, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

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

[Footnote added.]

CIP-003-3 R4

CIP-003-3 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-002-3, 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. (Retirement approved by NERC BOT pending applicable regulatory approval.)
> >
> > 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-003-3 R4 has a "Medium" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-003-3 R4 to the Regions. URE discovered information that it should have classified as CCA information. Specifically, URE discovered that the tickets in its change control systems were not identified as CCA information.

The Regions determined that URE had a violation of CIP-003-3 R4 for failing to implement its program to identify, classify, and protect information associated with CCAs.

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

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-003-3 R4 has the potential to affect the reliable operation of the BPS by increasing the likelihood of inappropriate access to CCA information. The risk to the reliability of the BPS was mitigated by the following factors. None of URE's CCA information repositories are publicly available, and all require some level of electronic or physical access protection. URE controls access by corporate level security standards, and access is limited to URE employees, contractors, or third-party suppliers with authorized access. URE requires all URE employees with authorized access to business records to undergo annual training regarding the appropriate use, handling, and retention of those records.[5]

CIP-003-3 R5

CIP-003-3 R5 provides in pertinent part:

> R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> ***
>
> 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-003-3 R5 has a "Lower" VRF and a "Severe" VSL.

During Reliability*First*'s Compliance Audit, of URE1, Reliability*First* discovered a violation of CIP-003-3 R5. Three months prior to the Compliance Audit, URE2 submitted a Self-Report to SERC identifying a violation of CIP-003-3 R5. URE's documentation of its annual review of access privileges did not

[5] Business records are broader than CCA information but include CCA information.

include access privileges or links to defined or approved roles. The documentation does not clearly delineate which individuals are assigned to which roles or which access rights are provided to those individuals. As a result, URE failed to confirm that the access privileges to protected information correspond with its needs and appropriate personnel roles and responsibilities, as required by CIP-003-3 R5.2.

In conjunction with URE's enterprise processes, URE also utilizes business-unit specific processes to control and manage access to CCA information. Upon review of the processes, Reliability*First* discovered that URE failed to assess annually and document the processes for controlling access privileges to CCA information. In instances where the process had a revised version history indicating annual review, it was unclear what URE assessed during the annual review. Reliability*First* reviewed seven procedures that pertain to controlling access privileges to protected information. Each of these procedures had a deficiency whereby URE failed to demonstrate that it had annually assessed the processes for controlling access privileges to protected information, as required by CIP-003-3 R5.3.

The Regions determined that URE had a violation of CIP-003-3 R5 for failing to: 1) ensure that the access privileges to protected information are correct and that they correspond with URE's needs and appropriate personnel roles and responsibilities; and 2) annually assess the processes for controlling access privileges to protected information.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, excessive or unauthorized access to URE's system increases the likelihood of disruptive acts, up to and including the loss of a substation. Furthermore, if the correct processes are not in place to control access to protected information, URE cannot be certain that protected information is properly secured. The risk to the reliability of the BPS was mitigated by the following factors. Access to all information requires some level of authorized electronic or physical access. URE has restricted access to CCA information repositories that it has identified. URE limits access to only those individuals that have a business need to access the information. URE typically controls access to electronic repositories not identified as CCA information by limiting electronic access to only those who are members of the appropriate directory service group and by limiting physical access to only those with access badges.

CIP-003-3 R6

CIP-003-3 R6 provides:

> R6. 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 SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-003-3 R6. Approximately a month prior to its Compliance Audit, URE1 self-reported a violation of CIP-003-3 R6 to Reliability*First*. URE failed to provide evidence that it documented all entity or vendor-related changes to hardware and software components of 60.04% of its CCAs pursuant to the change control process. In addition, during Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered several instances where URE's business units failed to follow the change control process.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-003-3 R6. URE2 self-reported a violation of CIP-003-3 R6 to SERC. URE failed to establish and document a process of configuration management for adding, modifying, replacing, or removing CCA hardware or software.

The Regions determined that URE had a violation of CIP-003-3 R6 for failing to: 1) document all entity or vendor-related changes to hardware and software components of CCAs pursuant to the change control process; and 2) establish and document a process for configuration management and implementation of supporting configuration management activities.

The Regions determined the duration of the violation from both the SERC and Reliability*First* Compliance Audits to be from the date the Standard became mandatory and enforceable as to URE through when URE completed its Mitigation Plan.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, configuration management ensures the network and environment are properly managed with consistent versions and settings so that the environment remains secure.

Insufficient implementation and support of configuration management can introduce unwanted security vulnerabilities, unauthorized access points, and impact the availability of critical systems up to and including the BPS. The risk posed to the reliability of the BPS was mitigated by the following factors. The testing process for two of URE's functions performed a staged implementation in development environments prior to implementing the changes, and URE periodically tested some security controls. Each business unit has a change control process that aligns with a change control process specified at the enterprise level. URE built configuration management processes into the overall change control process although URE failed to identify them. URE has change management systems in place to manage any changes that would introduce new Cyber Assets into the ESP and the addition of new access points to the ESP. If any changes were significant, with the exception of the violations discussed herein, URE conducted security controls testing including verification of ports and services, patching, and account management.

CIP-004-3

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. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3.

CIP-004-3 R4 provides:

> R4. Access — The Responsible Entity shall maintain list(s) of personnel with authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including their specific electronic and physical access rights to Critical Cyber Assets.
>
> > R4.1 The Responsible Entity shall review the list(s) of its personnel who have such access to Critical Cyber Assets quarterly, and update the list(s) within seven calendar days of any change of personnel with such access to Critical Cyber Assets, or any change in the access rights of such personnel. The Responsible Entity shall ensure access list(s) for contractors and service vendors are properly maintained.

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

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

URE2 self-reported a violation of CIP-004-3 R4 to SERC. URE2 mistakenly granted access to CCAs to an employee who had cybersecurity training and a valid PRA, but had not been approved for authorized cyber or authorized unescorted physical access to those CCAs. URE2 discovered the violation and URE2 revoked access three days after discovery. A cleaning contract employee no longer required authorized unescorted physical access to areas containing CCAs because the contractor relocated the employee to a different URE facility. URE2 failed to revoke the contract employee's physical access within seven calendar days. Approximately a month and half after the contractor no longer required authorized unescorted physical access URE2 revoked the contract employee's access.

The Regions determined the duration of the violation to be from the date URE2 granted access to the employee at issue through when URE2 revoked access to the employee at issue. The Regions determined the duration of the violation related to the contractor to be from the date URE2 was required to revoke access to the cleaning contract employee through when URE2 revoked access to the cleaning contract employee.

URE1 self-reported a violation of CIP-004-3 R4 to Reliability*First.* An URE1 employee's responsibilities changed, and as a result, the employee no longer required authorized cyber access to URE1's CCAs, including URE1's Energy Management System. URE1 failed to revoke the employee's access within seven calendar days. URE1 revoked the employee's access eight days after the employee no longer required authorized cyber access.

The Regions determined the duration of the violation to be from the date URE1 was required to revoke the employee's access through the date URE1 revoked the employee's access.

URE1 self-reported a violation of CIP-004-3 R4 to Reliability*First*. An URE1 student co-op's assignment ended, and as a result, the student no longer required authorized unescorted physical access to a site containing CCAs. URE1 failed to revoke the student's access within seven calendar days. URE1 revoked the student's access night days after the student co-op no longer required authorized unescorted physical access.

The Regions determined the duration of the violation to be from the date URE1 was required to revoke the student's access through the date URE revoked the student's access.

URE2 self-reported a violation of CIP-004-3 R4 SERC. An URE2 employee resigned, and as a result, the employee no longer required authorized unescorted physical access to a site containing CCAs. URE2 failed to revoke the employee's access within seven calendar days. URE2 revoked the employee's access twelve days after the employee no longer required authorized unescorted physical access.

The Regions determined the duration of the violation to be from the date URE2 was required to revoke the employee's access through the date URE revoked the employee's access.

URE1 self-reported a violation of CIP-004-3 R4 to Reliability*First*. An URE1 intern's assignment ended, and as a result, the intern no longer required authorized unescorted physical access to a site containing CCAs. URE1 failed to revoke the intern's access within seven calendar days. URE1 revoked the intern's access eleven days after the intern no longer required authorized unescorted physical access.

The Regions determined the duration of the violation to be from the date URE was required to revoke the intern's access to the date URE revoked the intern's access.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional violation of CIP-004-3 R4. URE2 self-reported a violation of CIP-004-3 R4 to SERC. For the year prior to the Audit, URE failed to provide evidence that it reviewed the specific access rights of all individuals as part of the quarterly access review process and failed to provide evidence that it updated the access lists within seven calendar days across all of its business units, as required by CIP-004-3 R4.1.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that URE had a violation of CIP-004-3 R4 for failing to: 1) review the list of its personnel who have authorized cyber or authorized unescorted physical access to CCAs and update the list within seven days of any change of personnel with such access to CCAs or any change in the access rights of such personnel; and 2) revoke authorized cyber and authorized unescorted physical access to a CCA within seven days for individuals who no longer required such access.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. All individuals at issue had valid PRAs and cybersecurity training. None of the individuals at issue used their access rights after URE was required to revoke their access. One of the individuals remained a URE employee, and one of the individuals remained a contractor for URE. In addition, for the employee at issue in the fourth Self-Report, URE2 revoked the employee's badge, reducing the likelihood that the employee could gain access to the site.

CIP-005-3

The purpose statement of Reliability Standard CIP-005-3 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-005-3 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-005-3.
> >
> > R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003-3; Standard CIP-004-3 Requirement R3; Standard CIP-005-3 Requirements R2 and R3; Standard CIP-006-3 Requirement R3; Standard CIP-007-3 Requirements R1 and R3 through R9; Standard CIP-008-3; and Standard CIP-009-3.

CIP-005-3 R1 has a "Medium" VRF and a "Severe" VSL.

CIP-005-3 R1.1

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-005-3 R1.1. URE1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-005-3 R1.1 in Reliability*First.* As a cybersecurity measure, URE employs devices in its intrusion detection and prevention system that communicate to a sensor. One interface is connected outside the ESP, and the other interface is connected inside the ESP. URE failed to identify and document these devices as access points to the ESPs, as required by CIP-005-3 R1.1.

In addition, during Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional violation of CIP-005-3a R1.1. URE1 failed to identify certain network switches that are configured to switch traffic to multiple virtual local area networks (LANs). Certain of these networks contain CCAs that reside in ESPs, and other networks do not reside within ESPs. Because these switches serve both trusted and non-trusted networks with the same hardware, these switches are access points to the ESP. URE1 failed to identify and document these access points to the ESP.

Reliability*First* determined that URE had a violation of CIP-005-3 R1.1 for failing to identify a Cyber Asset as an access point to the ESP.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, an unidentified access point to the ESP can provide information about internal ESP traffic to unauthorized personnel. If the device or an upstream network device is incorrectly configured, it can provide potential unauthorized access into the ESP. The risk to the reliability of the BPS was mitigated by the following factors. The network switches are configured with virtual LANs that logically separate the ESP networks from the non-ESP networks, reducing the likelihood of unauthorized traffic entering the ESP through the network switch from a virtual LAN not established within the ESP. In addition to site physical security, all devices were located within a PSP. URE protected and restricted access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group. The individuals administering all devices at issue had URE-specific cybersecurity training as well as updated PRAs.

CIP-005-3 R1.4

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-005-3 R1.4. During the site visit to a Control Center, Reliability*First* discovered a server that was a non-critical Cyber Asset within a defined ESP that URE1 had not identified and protected pursuant to CIP-005-3, as required by CIP-005-3 R1.4.

The Regions determined that URE had a violation of CIP-005-3 R1.4 for failing to identify and protect a non-critical Cyber Asset within a defined ESP.

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

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE performed test procedures on the applicable device prior to its introduction into the ESP. Within the ESP, URE performed patching for antivirus signatures and monitored the devices for security events. URE granted access only to those individuals who had cybersecurity training and valid PRAs. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-005-3 R1.5

URE1 self-certified non-compliance with CIP-005-3 R1.5 to Reliability*First*. In addition, during Reliability*First*'s Compliance Audit of URE1, Reliability*First* identified an additional instance of this violation. URE1 submitted a Self-Report to SERC identifying a violation of CIP-005-3 R1.5. URE's Cyber Assets used in the access control and/or monitoring of the ESP are its electronic access control and monitoring (EACM) devices. URE discovered that it failed to identify all EACM devices. Specifically, URE failed properly to identify and therefore afford the protections of: CIP-003 R4, R5, and R6; CIP-004 R3; CIP-005 R2 and R3; CIP-006 R3; CIP-007-3 R1 and R3 through R9; and CIP-009 R1 through R5 for the following devices: 1) the directory service domain devices (used for user access management for most EACM devices); 2) the access control server (used for authentication and authorization of network devices); 3) the network automation devices (used for monitoring); 4) the network node manager devices (used for monitoring); and 5) the RSA appliances (used to authenticate users).

In addition, URE failed to afford certain of the protections required by CIP-005-3 R1.5 to certain of its EACM devices. Specifically, URE failed to afford the protections of: CIP-005 R2 and R3; CIP-007-3 R3,

R5, R6, and R9; and CIP-009 to its terminal access servers, which are used to control remote access to network devices within the ESP and the primary access point to the ESP. Furthermore, URE failed to afford the protections of CIP-006 R3 and CIP-007-3 R1, R3, R6, and R8 to its devices, which are used for security event logging for devices within certain network domains.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, although URE identified no compromise to any CCAs, the potential for such compromise existed. A violation of CIP-005-3 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity for cyber intrusions to occur on CCAs located outside an established ESP. The risk to the reliability of the BPS was mitigated by the following factors. The devices at issue were subject to URE's cybersecurity policies and procedures pursuant to CIP-003-3 R1, R2, and R3, and CIP-008-3. The individuals administering all devices at issue had URE-specific cybersecurity training as well as updated PRAs.

CIP-005-3 R2

CIP-005-3 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.
>
> ***

> R2.4. Where external interactive access into the Electronic Security Perimeter has been enabled, the Responsible Entity shall implement strong procedural or technical controls at the access points to ensure authenticity of the accessing party, where technically feasible.

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

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-005-3a R2. URE1 submitted a Self-Report identifying the same violation of CIP-005-1 R2 in Reliability*First*. At its electronic access points to the ESP, URE failed to enable only the ports and services required for operations and for monitoring Cyber Assets within the ESP, as required by CIP-005-3 R2.2. Specifically, URE's firewall rules indicated broad destinations and port ranges not required for operations or for monitoring Cyber Assets within the ESP. In addition, during the Compliance Audit, SERC discovered that at two sites and a control center, URE2 had several firewall rules in place allowing interactive access traffic to enter the ESP that allowed interactive access traffic into the ESPs without authenticating to the remote access architecture.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, access points to the ESP that are configured too broadly may allow unnecessary traffic into or out of the ESP, and these additional routes may be used to disrupt CCA operations or allow unauthorized traffic into the ESP. The risk to the reliability of the BPS was mitigated by the following factors. URE had in place certain controls such as firewall rules that denied access by default and specific user account requirements that decreased the likelihood of unauthorized access. In addition, URE has user account requirements in place on all Cyber Assets within the ESP, except as identified in violations discussed herein. These requirements state that no individual may be granted electronic access to a Cyber Asset until that individual has received appropriate training, background screening, and authorization. These individuals must set passwords that conform to the complexity requirements of the CIP Standards. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-005-3a

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 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-005-3a R3 has a "Medium" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-005-3a R3. URE1 performed maintenance for 91 minutes on its intrusion detection system that required an outage of the intrusion detection system. There is no fail-over mechanism to perform monitoring during an outage of the intrusion detection system, and as a result, URE1 failed to implement its process for monitoring access at access points to the ESP 24 hours a day, seven days a week.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional instance of non-compliance with CIP-005-3a R3. For one of its access points to the ESP at one of its switchyards, URE1's router produced no logs for a month. This router was not logging pursuant to URE1's process

for logging access at an access point to an ESP. The router was producing logs, but URE's tool for aggregating logs was not receiving the produced logs.

The Regions determined that URE had a violation of CIP-005-3a R3 for failing to: 1) implement its process for monitoring access at an access point to an ESP 24 hours a day, seven days a week; and 2) implement its process for logging access at an access point to an ESP.

The Regions determined the duration of the violation related to the intrusion detection system to be 91 minutes, the time during which the intrusion detection system was not operational.

The Regions determined the duration of the violation related to URE1's switchyard to be from when the date the entity was required to comply with the Standard and was required to comply with CIP-005 through when URE completed its Mitigation Plan.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-005-3a R3 has the potential to affect the reliable operation of the BPS by providing the opportunity for individuals to access an entity's ESP while leaving no record of the intrusion. Without having monitoring processes in place at access points, an entity would be unable to detect and alert for unauthorized access to its ESP. Therefore, an entity would be unable to prevent or track intrusions that could result in harm to the integrity of CCAs within the ESP. The risk to the reliability of the BPS was mitigated by the following factors. URE had in place additional monitoring during the outage of the intrusion detection system including logging of all access points to the ESP. In addition, URE notified the affected telecommunications groups, server support groups, and system operations coordinators to ensure those groups reported any suspicious activity or events immediately. URE provides training on the availability of incident response plans to everyone with access to CCAs, prior to being granted access. The individuals involved in the incident response process participate in annual drills to reinforce the initial training. URE discovered no unauthorized attempts at or actual unauthorized access to the ESP during the duration of this violation.

CIP-005-3a R4[6]
CIP-005-3a R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R4.2 A review to verify that only ports and services required for operations at these access points are enabled;
>
> ***
>
> R4.5 Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

CIP-005-3a R4 has a "Medium" VRF and "Severe" VSL.

URE1 self-certified non-compliance with CIP-005-3a R4 to Reliability*First*.[7]

URE2 submitted a Self-Report to SERC identifying a violation of CIP-005-3a R4. URE2 performed cyber vulnerability assessments (CVAs) of the electronic access points to the ESP; however, URE2 discovered that it failed to include a complete review of its routers to verify that only ports and services required for operations at access points were enabled. URE's additional review extended past the year, and as a result, URE failed to perform a complete review of ports and services for the year prior to when URE2 submitted its Self-Report, as required by CIP-005-3a R4.2.

[6] This violation spans versions 3 through 3a of the Standard. For ease of reference, version 3a will be used throughout this document.
[7] In its Self-Certification, URE1 also identified a possible violation of CIP-005-3a R4.5 because it failed to document an action plan to remediate or mitigate vulnerabilities identified in the assessment. URE1 identified no vulnerabilities during its cyber vulnerability assessments, however, so it was not required to document an action plan. As a result, Reliability*First* is not proceeding with that possible violation of CIP-005-3a R4.5.

URE1 submitted a Self-Report to Reliability*First* identifying an additional instance of non-compliance with CIP-005-3a R4. URE1 performed CVAs of the electronic access points to the ESPs; however, URE1 failed to include 13 firewalls and 10 routers in those assessments. URE1's review extended past the year, and as a result, URE1 failed to perform a complete review of ports and services for the year, as required by CIP-005-3a R4.2. In addition, URE failed to document the results of the assessment, as required by CIP-005-3a R4.5.

Both of these issues occurred because URE failed to schedule enough time to perform the ports and services review and the action plan to remediate vulnerabilities identified in the assessment.

In addition, in its review of ports and services, URE performed a review of only unused firewall rules to determine whether URE could remove them from the system. However, URE failed to perform a review of its used firewall rules, in violation of CIP-005-3 R4.2. Furthermore, for three of its functions' routers only, URE performed a review of only 3.05% of its ports in Reliability*First* and 1.53% of its ports in SERC rather than a review of all of its ports in the year, as required by CIP-005-3a R4.2.

The Regions determined that URE had a violation of CIP-005-3a R4 for failing to include in its CVA a complete review to verify that only ports and services required for operations at access points are enabled and documentation of the results of the CVA.

The Regions determined the duration of the violation regarding the CVA for URE2 to be from the date URE documented its CVA through when URE completed the full scan.

The Regions determined the duration of the violation regarding the CVA for URE1 to be from the date URE documented its CVA through when URE completed its Mitigation Plan.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-005-3a R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for individuals to exploit vulnerabilities of an entity's ESP access points of which the entity is unaware. By exploiting vulnerabilities which would have been discoverable and preventable through the application of an annual CVA, an individual may gain unauthorized access CCAs within the ESP and cause harm to the integrity of the CCAs.

The risk to the reliability of the BPS was mitigated by the following factors. URE afforded these routers the requisite protections of CIP-005 and CIP-007, except where a violation is discussed herein. For CIP-005 those include the ESP, electronic access controls, monitoring electronic access, CVA, and

documentation review and maintenance. For CIP-007-3 those include test procedures, disabling ports and services, security patch management, malicious software protection, account management, security status monitoring, and disposal or redeployment. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-005-3 R5

CIP-005-3 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-005-3.
>
> > R5.1. The Responsible Entity shall ensure that all documentation required by Standard CIP-005-3 reflect current configurations and processes and shall review the documents and procedures referenced in Standard CIP-005-3 at least annually.
> >
> > ***
> >
> > R5.3. The Responsible Entity shall retain electronic access logs for at least ninety calendar days. Logs related to reportable incidents shall be kept in accordance with the requirements of Standard CIP-008-3.

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

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-005-3 R5. For one Cyber Asset that supports the control center, URE1 failed to retain electronic access logs for 90 calendar days, as required by CIP-005-3 R5.3. Instead, URE1 retained electronic access logs for 86 calendar days only. URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-005-3 R5. URE1 failed to review one document at one of its facilities, ESP document, as required by CIP-005-3 R5.1.

The Regions determined that URE had a violation of CIP-005-3 R5 for failing to: 1) review annually one document as required by CIP-005-3; and 2) retain electronic access logs for at least 90 calendar days.

The Regions determined the duration of the violation for failure to retain electronic access logs to be from when the Standard became mandatory and enforceable as to URE a through when URE completed its Mitigation Plan.

The Regions determined the duration of the violation related to the ESP document to be from the date by which URE1 was required to review the document to the date URE1 reviewed the document.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Logs were available for 86 calendar days for the Cyber Asset. The logs were available for a large percentage of the time required, reducing the likelihood that missing logs would have occurred. In addition, URE made no changes to the content of the ESP document during the prior year. URE makes changes to the ESP itself and then updates this document accordingly. The fact that URE made no changes indicates that there were no changes to the ESP during the prior year.

CIP-006-3

The purpose statement of Reliability Standard CIP-006-3 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-006-3 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. All Cyber Assets within an Electronic Security Perimeter shall reside within an identified Physical Security Perimeter. Where a completely enclosed ("six-wall") border cannot be established, the Responsible Entity shall deploy and document alternative measures to control physical access to such Cyber Assets.
> >
> > ***
> >
> > R1.4. Appropriate use of physical access controls as described in Requirement R4 including visitor pass management, response to loss, and prohibition of inappropriate use of physical access controls.

***

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

***

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

***

R1.8. Annual review of the physical security plan.

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

CIP-006-3 R1.1

URE1 self-certified non-compliance with CIP-006-3 R1 to Reliability*First*. During the installation of a shower room at a station, the individuals routing a heating, ventilation, and air conditioning connection cut a hole above the drop ceiling tiles that measured 104 square inches. URE1 failed to identify this 104 square inch hole as a physical access point in its physical security plan, as required by CIP-006-3 R1.1.

The Regions determined that URE had a violation of CIP-006-3 R1.1 for failing to ensure all Cyber Assets within an ESP reside within an identified PSP.

The Regions determined the duration of the violation to be from the date the hole was cut in the ceiling through when URE1 closed the opening.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Security staff monitors the location 24 hours a day, seven days a week, decreasing the likelihood that an unauthorized user could gain access to URE1's system. In addition,

the opening was less accessible due to its location above a drop ceiling, and it was not visible as an entry point. Furthermore, URE1 has no evidence that anyone entered the site through this opening. URE1 maintained a site-specific physical security plan that provided lower-level details available to the personnel at the site, including the key program. Also, URE1 stores all PSP diagrams, whether on electronic or physical media, in a secure location with limited access, and URE1 only provides drawings to those who need to know. URE stores these PSP diagrams in accordance with its CCA information policies. URE1 was also monitoring and controlling physical access to the PSPs during the duration of the violation. In addition to the key program being documented within the site-specific physical security plan, the key program was also a topic during the annual training that the individuals with regular access to the site received.

URE2 submitted a Self-Report to SERC identifying a violation of CIP-006-3 R1. During its periodic site inspection, URE2 discovered an opening in the PSP wall at a substation control house. The opening was in the wall between the utility room outside the PSP and a vacant room inside the PSP. URE2 used a contractor to replace a heating duct with a smaller conduit, leaving an opening where the duct once was. The opening was approximately 176 square inches, and URE2 sealed the opening the date it discovered the opening.

The Regions determined that URE had a violation of CIP-006-3 R1.1 for failing to ensure all Cyber Assets within an ESP reside within an identified PSP. The Regions determined the duration of the violation to be from the date URE2 replaced the duct through when URE2 sealed the opening.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-006-3 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to access Cyber Assets that are not protected by the implementation of a physical security plan. The risk to the reliability of the BPS was mitigated by the fact that the control house is located inside the secured fence area of the substation, and the utility room can only be accessed by an exterior door that is normally locked with no access to the inside of the PSP. In addition, access to the vacant room adjacent to the utility room is through one of four CIP-secured doors located in other areas of the control house. URE controls access to the PSP through login and logout procedures. There is barbed wire fencing around the substation along with a locked gate. In addition, the opening was small and not easily accessible, decreasing the likelihood of unauthorized access through it. Furthermore, URE2 has well-defined criteria for creating a six-wall border, but failed in this instance to ensure the construction personnel fully understood those criteria.

URE2 submitted a Self-Report to SERC identifying an additional violation of CIP-006-3 R1. URE2 discovered two Cyber Assets within the ESP at a substation that were located outside of the associated PSP. URE2 failed to submit a Technical Feasibility Exception (TFE) for these devices and failed to apply compensating measures.

The Regions determined that URE had a violation of CIP-006-3 R1.1 for failing to ensure all Cyber Assets within an ESP reside within an identified PSP.

The Regions determined the duration of the violation to be from the date URE2 installed the first device through when URE closed the opening.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-006-3 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to access Cyber Assets that are not protected by the implementation of a physical security plan. The risk to the reliability of the BPS was mitigated by the fact that URE2 strictly controls access to the ESP, and the devices resided within a secured physical substation perimeter consisting of locked gates and a secured control house. In addition, the devices at issue had secure and complex passwords and are serially connected with no Internet Protocol or routable protocols enabled.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-006-3 R1. URE2 submitted a Self-Report to SERC identifying a violation of CIP-006-3 R1.1. Reliability*First* discovered a two foot-by-two foot opening above a raised ceiling in an URE operations center PSP. As a result, URE failed to ensure that the Cyber Assets within the ESP resided in a PSP as required by CIP-006-3 R1.1.

The Regions determined that URE had a violation of CIP-006-3 R1.1 for failing to ensure all Cyber Assets within an ESP reside within an identified PSP.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through when URE closed the opening.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE operations personnel monitor the PSP 24 hours a day, seven days a week, and security staff routinely guards it. This PSP is wholly located within a secured corporate building that is non-public and requires badge access or escort by a badged employee. In addition, all devices

were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-006-3 R1.1. URE1 conducted a Spot Check of an operations center. URE1 discovered a gap in the six-wall border of PSP exceeding 96 square inches above a suspended ceiling in the operations center energy management room. The opening was in the corner of a room where several ducts, conduits, cable trays, structural beams, and a side wall prevented viable access.

The Regions determined that URE had a violation of CIP-006-3 R1.1 for failing to ensure all Cyber Assets within an ESP reside within an identified PSP.

The Regions determined the duration of the violation to be from J the date the Standard became mandatory and enforceable as to URE through when URE1 closed the opening.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of BPS. The risk to the reliability of the BPS was mitigated by the following factors. The opening was in the corner of a room where several ducts, conduits, cable trays, structural beams, and a side wall prevented viable access. In addition, the PSP wall area is within an operations center building that has perimeter fencing, onsite contract security, card-access controlled fence gates, and card-access controlled building access. Furthermore, the operations center is a control center manned 24 hours a day, seven days a week by URE personnel. These factors reduce the likelihood of unauthorized physical access to this site through the identified opening.

CIP-006-3 R1.4

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional violation of CIP-006-3 R1. URE2 submitted a Self-Report to SERC identifying a violation of CIP-006-3 R1. URE utilizes a restricted key process as a backup physical access control, which constitutes a physical access control pursuant to CIP-006-3 R4. URE, however, failed to include information regarding the restricted key backup process in its physical security plan, as required by CIP-006-3 R1.4.

The Regions determined that URE had a violation of CIP-006-3 R1.4 for failing to include appropriate use of certain physical access controls in its physical security plan.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The keys at issue still work when the primary access control is unavailable. In the event that the physical access control system is not working, individuals can use the key with the restricted key system to gain authorized entry into the PSP. Using a key generates an alarm that is displayed at the security console. The key is considered a backup because URE trains its employees that the badge is the primary means of access control and the keys are reserved for those PSPs that do not have a badge access control, or for entry into a PSP when the primary means of access is unavailable. This usage detail is located in the physical security plan.

URE has several protections in place that reduce the risk to reliability of the BPS. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-006-3 R1.6.2

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-006-3 R1. URE1 failed to implement its policy for continuously escorting visitors by allowing two people without authorized unescorted physical access to be unescorted in a PSP, as required by CIP-006-3 R1.6.2.

The Regions determined that URE had a violation of CIP-006-3 R1.6.2 for failing continuously to escort visitors within a PSP.

The Regions determined the duration of the violation to be one day the date the visitors were unescorted.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-006-3 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to access Cyber Assets that are not protected by the implementation of a physical security plan. The two unescorted individuals have NERC cybersecurity training and PRAs. In addition, these individuals had previously completed work inside the PSPs.

CIP-006-3 R1.8

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional violation of CIP-006-3 R1. Three months prior to the Compliance Audit, URE2 submitted a Self-Report to SERC identifying a violation of CIP-006-3 R1. URE's physical security plan references numerous documents that contain the detailed information illustrating compliance with CIP-006. URE required annual review of the physical security plan and left annual review of the documents referenced by the physical security plan to the discretion of the business unit managers. While URE annually reviewed the physical security plan document, URE failed to ensure annual review of the documents referenced by the physical security plan, as required by CIP-006-3 R1.8.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-006-3 R1 has the potential to affect the reliable operation of the BPS by providing the opportunity to access Cyber Assets that are not protected by the implementation of a physical security plan. URE has several protections in place that reduce the risk to reliability of the BPS. URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-006-3 R2

CIP-006-3 R2 provides in pertinent part:

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

***

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

URE self-certified non-compliance with CIP-006-3 R2 to Reliability*First*. URE submitted a Self-Report to SERC identifying a violation of CIP-006-3 R2. URE discovered that it failed to provide protections to certain of its physical access control and monitoring (PACM) devices, which are Cyber Assets that authorize and/or log access to the PSP. Specifically, URE provided the protective measures required by CIP-006-3 R2.2 only to its PACM server. Moreover, URE failed to provide the full range of protective measures required by CIP-006-3 R2.2 to its PACM server. Specifically, URE failed to provide the protective measures of: CIP-005-3 R2 and R3; CIP-007-3; CIP-008-3; and CIP-009-3 to the PACM server.

In addition, URE failed to identify and therefore provide the Cyber Assets that authorize and/or log access to the PSP that URE had not identified as such with any of the protective measures specified by CIP-006-3 R2.2. URE determined that certain of its devices also constituted Cyber Assets that authorize and/or log access to the PSP, and as such, it should have been providing the protective measures as required by CIP-006-3 R2.2 to these devices. URE failed to identify and therefore provide protective measures to 52 Cyber Assets that authorize and/or log access to the PSP.

The Regions determined that URE had a violation of CIP-006-3 R2 for failing to afford the requisite protections to all Cyber Assets that authorize and/or log access to the PSP.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to afford the majority of protective measures to its PACM server and its failure to afford any protective measures to the remainder of its PACM devices allowed for the potential compromise of CCAs. The risk to the reliability of the BPS was mitigated by the following factors. In the event that the PACM fails to operate, URE has in place alternative measures for the appropriate access to facilities using keyed locks and a protected key system. If this event occurs, the access points remain locked and there are manual processes in place for monitoring and logging access. To decrease the likelihood of inappropriate access in the event of a failure of the

PACM, the PACM components will not allow access to cards not previously accessed and cached in local memory.

CIP-006-3 R4

CIP-006-3 R4 provides:

> R4. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> • Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
>
> • Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
>
> • Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
>
> • Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-3 R4 has a "Medium" VRF and a "Severe" VSL.

URE1 self-certified non-compliance with CIP-006-3c R4 to Reliability*First*. URE1 utilizes a key system at one of its facilities, to control physical access. URE1 created 10 keys for the site, but URE1 was only tracking seven of them.[8] URE1 did not keep adequate records regarding the quantity of keys produced or to whom URE1 provided keys for these three keys, and as a result, URE1 failed to implement adequately the "Card Key" physical access method to the PSP.

The Regions determined that URE had a violation of CIP-006-3 R4 for failing to implement certain operational and procedural controls to manage physical access at an access point to a PSP 24 hours a day, seven days a week.

[8] While URE1 was able to contact the key provider and receive a verbal confirmation of the number of keys produced, no evidence was available to confirm this.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through when URE1 re-cored all impacted locks and replaced all the keys.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, URE's failure to control physical access to the station in this way increased the likelihood of unauthorized access. The risk to the reliability of the BPS was mitigated by the following factors. The primary means of access to the PSP, the badge system, was fully functional during the time period of the violation. Only individuals with valid PRAs and cybersecurity training had authorized access for coded badges allowing authorized unescorted physical access to the PSP. For the known quantity of keys, URE kept records regarding to whom keys were assigned and who therefore had access to the PSP. There is no ability to access the EMS from any of the Cyber Assets located within the ESP at the station through a deny-by-default rule set. URE monitors the PSP 24 hours a day, seven days a week from a security console, and the site is protected by a gated fence and security personnel patrol the site 24 hours a day, seven days a week.

CIP-006-3c R5
CIP-006-3c R5 provides:

> R5. Monitoring Physical Access —The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008-3. One or more of the following monitoring methods shall be used:
>
> • Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
>
> • Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R4.

CIP-006-3c R5 has a "Medium" VRF and a "Severe" VSL.

URE1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-006-3c R5. In addition, during Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered the same issue. URE1's procedures for addressing unauthorized access attempts state that if the number of unauthorized badge attempts reaches five within five minutes, the console operator will notify the primary and/or secondary site contacts. A vendor representative made more than five access attempts within five minutes with his access badge at one of URE1's control centers. URE1 had not coded the representative's access badge for access to any PSP. URE1 failed to review these unauthorized access attempts.

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-006-3c R5. URE1 discovered that due to software errors in its client monitoring system, URE1's system did not receive alarms to the monitoring console where it receives alarms related to unauthorized access attempts. The software errors occurred due to the migration of the monitoring console system from one version of an operating system to another. As a result, there was an alarm delivery delay for approximately five hours.

The Regions determined that URE had a violation of CIP-006-3c R5 for failing to review unauthorized access attempts immediately and by failing to monitor access points to the PSP.

The Regions determined the duration of the violation related to unauthorized badge attempts to be from the date URE1 failed to review the unauthorized access attempts through when URE completed its Mitigation Plan.

The Regions determined the duration of the violation related to software errors to be one day when URE1's system did not receive alarms to the monitoring console for approximately five hours.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, regarding the unauthorized badge attempts, URE1's console operator's failure to follow the procedures in this way increased the likelihood of unauthorized access. Regarding the software errors, this violation had the potential to affect the reliable operation of the BPS by providing the opportunity to access the PSP through inadequate technical and procedural controls to monitor physical access points. The risk to the BPS was mitigated by the following factors. Regarding the unauthorized badge attempts, the representative was attempting to make an office supply delivery within the PSP, unbeknownst to the representative. While the representative has a badge that allows general office access, the representative's badge was not authorized for entry into the PSP. The representative, an employee of a trusted and frequently-used vendor, appropriately filled

out the visitor log book. In addition, signage is clearly posted on the access doors stating that access is restricted and the identification badge must be specifically coded for access. Regarding the software errors, the following controls are in place at the substation at issue: a locked gate, security fencing including barbed wire, door controls, and frequent periodic inspections. In addition, when URE reviewed the logs, it discovered no unauthorized access attempts.

CIP-007-3

The purpose statement of Reliability Standard CIP-007-3 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-007-3 R1

CIP-007-3 R1 provides:

> 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-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> > R1.1. The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.
> >
> > R1.2. The Responsible Entity shall document that testing is performed in a manner that reflects the production environment.
> >
> > R1.3. The Responsible Entity shall document test results.

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

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-007-3 R1. A month prior to its Compliance Audit, URE1 submitted a Self-Report to Reliability*First* identifying a violation of CIP-

007-3 R1. URE1 submitted a Self-Report to Reliability*First* identifying an additional instance of a violation of CIP-007-3 R1. During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered the same violation. URE1 has in place cybersecurity test procedures to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls. For two its functions, however, URE1 failed to implement its cybersecurity test procedures for 60.43% of its CCAs and 44.17% of its Cyber Assets within the ESP, as required by CIP-007-3 R1. Specifically, for some firmware upgrades to Cyber Assets, URE1 failed to test for adverse effects on existing cybersecurity controls. In addition, for certain Cyber Assets, URE1's process failed to address the testing of ports and services during significant changes.

In addition, URE1 failed to document test results for security patches applied at one of its facilities. URE1 applied security patches to two CCAs and nine Cyber Assets within the ESP. URE1, however, failed to document test results ensuring that these significant changes to the existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls, as required by CIP-007-3 R1.3.

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-007-3 R1. URE1 discovered that a URE1 engineer replaced four firewalls without following documented test procedures. The new model was not in the minimum security baseline, which URE had developed and tested, so the engineer used the vendor-provided configuration guide. URE1 had not tested the configuration guide in a manner that reflects the production environment, as required by CIP-007-3 R1.1. URE1 discovered this issue when the compliance team lead rejected the change form because it did not conform to the minimum security baseline.

The Regions determined that URE had a violation of CIP-007-3 for failing to: 1) ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP do not adversely affect existing cybersecurity controls; and 2) document test results.

The Regions determined the duration of the CIP-007-3 R1 violation to be from the date the Standard became mandatory and enforceable as to URE through when URE revised its testing procedures to ensure they provide adequate evidence.

The Regions determined the duration of the CIP-007-3 R1.3 violation to be from the date URE1 applied the security patches through when URE completed its Mitigation Plan.

The Regions determined the duration of the CIP-007-3 R1.1 violation to be from the date the engineer deployed the firewalls through the date URE1 tested the configuration in a manner that reflects the production environment.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, if an entity fails to test significant changes to verify the effect those changes have on the security controls, security vulnerabilities may occur on the Cyber Assets without the knowledge of the entity and without compensating measures in place. These vulnerabilities may allow unauthorized personnel the ability to disrupt the operation of the Cyber Asset or to gain command and control over the asset itself. The risk to the reliability of the BPS was mitigated by the following factors. Regarding the violation of R1, URE1 performed a staged implementation in development environments prior to production deployment. Regarding the violation of R1.3, the equipment manufacturer verified and functionally tested the security patches that URE1 applied prior to their application in the production environment. Regarding the violation of R1.1, after the engineer installed the firewalls, the engineer reviewed the ports and services to ensure they met enterprise guidelines. In addition, after reviewing the firewalls in a manner consistent with the production environment, URE1 discovered no issues. In addition to site physical security, all devices at issue were located within a PSP. URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-007-3 R2

CIP-007-3 R2 provides in pertinent part:

> R2. Ports and Services — The Responsible Entity shall establish, document and implement 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).

CIP-007-3 R2 has a “Medium” VRF and a “Severe” VSL.

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-007-3 R2. URE1 submitted a Self-Report to Reliability*First* identifying the same violation of CIP-007-3 R2 in Reliability*First*. During Reliability*First*'s Compliance Audit of URE1, Reliability*First* identified an additional instance of the violation of CIP-007-3 R2. URE1's processes for determining baseline ports and services did not adequately identify the ports and services required for normal and emergency operations. In addition, URE1's processes for testing for significant changes did not include changes to ports and services. As a result, the ports and services baselines were not immediately updated and URE1 left unnecessary ports and services enabled. Therefore, URE1 failed to enable only those ports and services required for normal and emergency operations, as required by CIP-007-3 R2.1. In addition, URE1 failed to disable ports and services not required for normal and emergency operations, including those used for testing purposes, prior to production use of certain Cyber Assets within the ESPs, as required by CIP-007-3 R2.2.

The Regions determined that URE had a violation of CIP-007-3 R2 for failing to: 1) enable only those ports and services required for normal and emergency operations; and 2) disable other ports and services including those used for testing purposes, prior to production use of all Cyber Assets inside the ESPs.

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

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R2 has the potential to affect the reliable operation of the BPS by providing the opportunity for infiltration of unauthorized network traffic into the ESP through ports and services that are not necessary for normal or emergency operations, but nevertheless remain enabled. The risk to the reliability of the BPS was mitigated by the following factors. URE1 had in place certain controls such as firewall rules that deny by default and specific user account requirements that decreased the likelihood of unauthorized access through non-required open ports. URE1 would have been able to detect and alert for infiltration of the ESPs through ports and services because one of the multiple layers of defense the URE employs is the implementation of intrusion detection and prevention system devices. These intrusion detection and prevention system devices are programmed to detect for malicious traffic attempting to gain access to the ESP, regardless of whether the ports and services are enabled on the end-device. If the intrusion detection and prevention system detects malicious traffic, it alerts and/or prevents the malicious traffic from gaining access to the ESP, depending on the specific technology at use in the ESP.

In addition to site physical security, all devices were located within a PSP. In addition, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-007-3 R3

The purpose of CIP-007-3 provides:

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

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

URE2 submitted a Self-Report to SERC identifying a violation of CIP-007-3 R3. URE submitted a Self-Report to Reliability*First* identifying a violation of CIP-007-3 R3. Pursuant to its security patch management program, URE considered only operating system security releases for Cyber Assets within the ESP managed by a systems group. URE1 failed to consider security patches or security upgrades to software installed on the Cyber Assets. As a result, URE failed to install some security patches and security upgrades on 60.04% of its CCAs and 43.07 of its Cyber Assets within the ESP in a timely manner, and in some instances, failed to do so at all.

The Regions determined that URE had a violation of CIP-007-3 for failing to: 1) establish a security patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for Cyber Assets within the ESP; 2) document the assessment of security patches and security upgrades for Cyber Assets within the ESP; and 3) document the implementation of security patches for Cyber Assets within the ESP.

URE determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through when URE revised its patch management program to monitor for all software-related security issues.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R3 has the potential to affect the reliable operation of the BPS by providing the opportunity for infiltration of unauthorized network traffic into the ESP when security patches and upgrades are not installed on Cyber Assets within the ESP. The risk to the reliability of the BPS was mitigated by the following factors. URE installed the requisite security patches and upgrades for the operating systems of these Cyber Assets. The Cyber Assets at issue have limited software installed, so there were few non-operating system security patches or security upgrades. In addition, the Cyber Assets were located within the ESP. URE is actively involved with software vendors, software security announcements, the Electricity Sector Information Sharing and Analysis Center (ES-ISAC), and other security forums where URE may become aware of security patches and other security patch risks. Furthermore, URE runs intrusion detection and intrusion prevention on the network to prevent the propagation of malware, and where possible, URE also runs host-based firewalls to provide additional protection against the propagation of malware. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-007-3 R4

CIP-007-3 R4 provides:

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

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

CIP-007-3 R4 has a "Medium" VRF and a "Severe" VSL. T

URE submitted Self-Reports to the Regions identifying a violation of CIP-007-3 R4. URE discovered 111 Cyber Assets within the ESP that require the use of antivirus software pursuant to CIP-007-3 R4. Fifty-eight of the Cyber Assets at issue were in the Reliability*First* region and 53 of the Cyber Assets at issue were in the SERC region. These devices are CCAs and Cyber Assets within the ESP that do not run an operating system capable of using antivirus software. URE misunderstood the applicability of the CIP-007-3 R4 to these devices and failed to submit a TFE. URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-007-3 R4. In addition to the above Cyber Assets, URE1 discovered 32 non-critical Cyber Assets within an ESP on which it was technically infeasible to install antivirus software and malware prevention tools. URE1 failed to submit a TFE. URE1 added 16 of these devices to production in the fall and the remaining 16 of these devices to production approximately two and half months later.

The Regions determined that URE had a violation of CIP-007-3 for failing to use antivirus software or submit a TFE for certain Cyber Assets within the ESP.

URE determined the duration of the first violation to be the date the Standard became mandatory and enforceable as to URE through when URE submitted a TFE. URE determined the duration of the second instance of the violation to be from the date URE1 added 16 of the devices to production, through when URE1 submitted a TFE.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R4 has the potential to affect the reliable operation of the BPS by providing the opportunity for the introduction, exposure, and propagation of malware on Cyber Assets within the ESP. The risk to the reliability of the BPS was mitigated by the following factors. The 111 devices at issue are either firmware devices or focused delivery software-driven devices with limited user interactions that involve the most exposure to viruses or other malware. None of the devices have direct connectivity with the Internet, and some devices are redundant to each other. The devices reside within the ESP, and logging and monitoring is in place for these devices, where technically feasible.

URE also has several protections in place that reduce the risk to reliability of the BPS. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group. The 32 non-critical Cyber Assets are located within an ESP and a PSP and have alarms back to the ESP console which is monitored 24 hours a day, seven days a week. In addition, only individuals with cybersecurity training and PRAs have access to these devices.

CIP-007-3 R5

CIP-007-3 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-003-3 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-003-3 Requirement R5 and Standard CIP-004-3 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-007-3 R5 has a "Lower" VRF and a "Severe" VSL.

CIP-007-3 R5

URE1 self-certified non-compliance with CIP-007-3 R5 to Reliability*First*. URE1 discovered a printer at a blackstart facility within the PSP and ESP that contained an administration account. URE1 failed to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access for this account, as required by CIP-007-3 R5. Specifically, URE1 failed to evaluate the printer for any accounts that have access to the printer, implement its account management policy, and monitor activity on this account.

The Regions determined that URE had a violation of CIP-007-3 R5 for failing to implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through when URE1 removed the printer from the ESP.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. For the administration account located on the printer, the printer resided behind a PSP and ESP. In addition, while the facility is a blackstart facility, a limited number of URE personnel have access to the facility due to infrequent use and maintenance (3.16% of individuals have access). In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-007-3 R5.3

URE2 submitted a Self-Report to SERC identifying a violation of CIP-007-3 R5 and URE1 provided additional information to Reliability*First* regarding its violation of CIP-007-3 R5. URE failed to submit TFEs for all of its devices managed in accordance with the directory service, which constitutes 1,326 devices, because those devices are technically incapable of implementing the password requirements of CIP-007-3 R5.3. Specifically, URE can require the criteria for these passwords, but there is no method of demonstrating that the individual employees were following the criteria.

URE submitted a Self-Report to the Regions identifying an additional violation of CIP-007-3 R5.3. URE discovered 52 CCAs and Cyber Assets within the ESP that require the use of passwords that meet the length and complexity requirements as specified in CIP-007-3 R5.3. These devices are non-server systems that do not run an operating system capable of using such passwords. However, URE misunderstood the applicability of CIP-007-3 R5.3 to these devices and failed to submit a TFE.

The Regions determined that URE had a violation of CIP-007-3 R5 for failing to submit a TFE for certain Cyber Assets that were not capable of using passwords as required by CIP-007-3 R5.3.

The Regions determined the duration of the first issue with R5.3 to be the date the Standard became mandatory and enforceable as to URE through when URE completed submitting TFEs. The Regions determined the duration of the second instance of the violation of R5.3 to be from the date the Standard became mandatory and enforceable as to URE through when URE submitted a TFE.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity for unauthorized system access. The risk to the reliability to the BPS was mitigated by the following factors. For the first issue with CIP-007-3 R5.3, URE has multiple layers of protection in place for these devices, including redundant firewalls and redundant intrusion detection system devices that protect the ESPs at both the primary control center and the backup control center. In addition, URE monitors all devices within the ESPs for security events, which ensure that workstations are not compromised without proper alerting in place. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group. In addition to site physical security, all devices were located within a PSP. The devices at issue have enabled access controls, security patches, change management program, antivirus software, and access point controls where technically feasible. For the second instance of the violation of CIP-007-3 R5.3, the assets at issue did require a password, although the passwords did not meet the length and complexity requirements of CIP-007-3 R5. In addition, the assets were located within an ESP.

CIP-007-3 R5.3.2

URE submitted a Self-Report to the Regions identifying an additional violation of CIP-007-3 R5. CIP-007-3 R5.3.2 requires that each password consist of a combination of alpha, numeric, and "special" characters. However, URE's password policy required its passwords to include any three of the following five character types: 1) English uppercase letters (A-Z); 2) English lowercase letters (a-z); 3) base 10 digits (0- 9); 4) non-alphanumeric; or 5) unicode characters. Therefore, URE failed to define the three criteria set forth in CIP-007-3 R5.3.2 as its criteria for passwords. This violation affects URE's entire set of password-protected assets for three of its functions.

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-007-3 R5. For four Cyber Assets, URE1 failed to submit a TFE because of the Cyber Assets' inability to support the password requirements of CIP-007-3 R5.3.2. URE1 implemented the compensating measures submitted in the TFE upon commissioning the Cyber Assets.

The Regions determined that URE had a violation of CIP-007-3 R5.3.2 for failing to require and use passwords that are a minimum of six characters, consist of a combination of alpha, numeric, and "special" characters, and are changed at least annually.

The Regions determined the duration of the first issue with CIP-007-3 R5.3.2 to be from the date the Standard became mandatory and enforceable as to URE through when URE revised its internal policy to comply with CIP-007-3 R5.3.2. The Regions determined the duration of the second instance of the violation of CIP-007-3 R5.3.2 to be from the date URE1 installed one of the devices when URE1 submitted a TFE.

The Regions determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Regarding the first issue with CIP-007-3 R5.3.2, although URE failed to utilize the password requirements set forth in CIP-007-3, R5.3.2, URE maintained criteria that resulted in complex passwords. In addition, all devices requiring passwords reside behind firewalls and routers that have restricted remote access. In addition, all devices requiring passwords reside within a PSP, which are accessible only by individuals who have had PRAs, cybersecurity training, and proper authorization to the PSPs. Regarding the second instance of the violation of CIP-007-3 R5.3.2, upon commissioning the Cyber Assets, URE implemented the following compensating measures. All devices reside within an ESP and PSP with alarming contacts back to the security console, which is monitored 24 hours a day, seven days a week. Only individuals who have had valid PRAs and cybersecurity training have access to these devices.

CIP-007-3 R5.2.3

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-007-3 R5. URE submitted a Self-Report to Reliability*First* identifying the same violation of CIP-007-3 R5 in Reliability*First*. Two of URE's functions failed to implement URE's corporate-wide policy to have an audit trail of the account use of shared accounts, as required by CIP-007-3 R5.2.3. This violation affected 34 shared accounts for the two functions.

The Regions determined that URE had a violation of CIP-007-3 R5.2.3 for failing to have an audit trail of the account use for certain shared accounts.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through when URE revised its internal policy to comply with CIP-007-3 R5.3.2.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, if the entity is unable to construct audit trails of the use of shared passwords, shared account activity may not be available to track back to a specific user. If a cybersecurity event occurred, the entity would be unable to construct audit trails to analyze the event

and its consequences. The risk to the reliability of the BPS was mitigated by the following factors. URE has policies in place to manage shared accounts that limit access to authorized individuals and provide steps to secure the account in the event of personnel changes. In addition, all individuals with access to the shared accounts at issue have cybersecurity training and PRAs in place. Furthermore, each of the systems at issue reside in PSPs.

CIP-007-3 R5.1.2, R5.1.3, R5.2.3, and R5.3

URE1 submitted a Self-Report to Reliability*First* identifying an additional instance of the violation of CIP-007-3 R5. URE1 did not have adequate inventory of the Cyber Assets with shared accounts and the accounts that existed for 18 CCAs and one non-critical Cyber Assets. As a result, URE1 failed to 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 90 days, as required by CIP-007-3 R5.1.2. For these 19 assets, URE1 failed to review user accounts annually to verify access privileges were in accordance with CIP-003-3 R5 and CIP-004-3 R4, as required by CIP-007-3 R5.1.3. In addition, for these 19 assets, URE1 failed to implement a policy for managing the use of shared accounts that limits access to only those with authorization, an audit trail of the account use, and steps for securing the account in the event of personnel changes, as required by CIP-007-3 R5.2.3.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered an additional instance of the violation of CIP-007-3 R5. First, URE1's method of generating logs for individual and system shared accounts does not allow the creation of historical audit trails of user account access activity. While URE1's log management system records all event logs, there is no method of interpreting those logs because it is unclear which data is the login or logout information. As a result, URE1 cannot generate a historical audit trail, as required by CIP- 007-3 R5.1.2.

Second, URE1 failed to configure the password controls for two Critical Cyber Assets pursuant to URE's password policy for two of its functions. Specifically, URE1 failed to require that users create passwords that are a minimum of six characters, consist of a combination of alpha, numeric, and "special" characters, and are changed at least annually, as required by CIP-007-3 R5.3.

The Regions determined that URE had a violation of CIP-007-3 R5.2.3 for failing to: 1) implement technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access; 2) have an audit trail of the account use for certain shared accounts; and 3) require and use passwords that are a minimum of six characters, consist of a combination of alpha, numeric, and "special" characters, and are changed at least annually.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE through the present. URE is scheduled to complete its Mitigation Plan at a future date.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity for unauthorized system access. The risk to the reliability of the BPS was mitigated by the following factors. In addition to site physical security, all devices were located within a PSP. In addition, URE1 protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-007-3 R6

CIP-007-3 R6 provides in pertinent part:

> 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.
>
> ***
>
> R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
>
> R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-3.
>
> R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.
>
> ***

CIP-007-3 R6 has a “Lower” VRF and a “Severe” VSL.

URE2 submitted a Self-Report to SERC identifying a violation of CIP-007-3 R6. URE2 had automatic logging enabled at a blackstart facility prior to when URE2 was required to comply with the standard. URE2 reassigned Internet Protocol addresses, inadvertently ceasing the log capture for the Cyber Assets within the ESP.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE2 through the date URE2 re-enabled the log capture that it had inadvertently suspended.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. In addition to site physical security, all devices were located within a PSP. In addition, URE2 protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

URE1 self-certified non-compliance with CIP-007-3 R6 to Reliability*First*. URE1 discovered that the printer at issue in the CIP-007-3 R5 violation described above, which was a Cyber Asset within the PSP and ESP at a blackstart facility, was incapable of implementing automated tools or organizational process controls to monitor system events related to cybersecurity, as required by CIP-007-3 R6. URE1 implemented automated tools and organizational process controls to monitor system events related to cybersecurity for all other Cyber Assets within the affected ESP; however, URE1 failed to submit a TFE for this printer.

The Regions determined the duration of this violation to be from the date the Standard became mandatory and enforceable as to URE1 to the date URE1 removed the printer from the ESP.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. For the administration account located on the printer, the printer resided behind a PSP and ESP. In addition, while the facility is a blackstart facility, a limited number of URE1 personnel have access to it.

URE submitted a Self-Report to the Regions identifying a violation of CIP-007-3 R6. URE discovered 90 CCAs and Cyber Assets within the ESP that require the implementation of automated tools or organizational process controls to monitor system events that are related to cybersecurity. These devices are non-server systems that do not run an operating system capable of implementing such security status monitoring. However, URE misunderstood the applicability of CIP-007 R6 to these devices and failed to submit a TFE.

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE to the date URE submitted a TFE.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. In addition to site physical security, all devices were located within a PSP. In addition, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

URE2 submitted a Self-Report to SERC identifying a violation of CIP-007-3 R6. URE submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-007-3 R6. URE failed to ensure that certain of its Cyber Assets within the ESP were maintaining logs of system events related to cybersecurity. Because the firewall policy configuration restricted data to one port which resulted in a blocking issue, and because the network switches were configured to send the logs to an incorrect server address for storage, 11 of URE's 17 network switches were not correctly transmitting log information of system events related to cybersecurity. Therefore, URE failed to issue automated or manual alerts for detected Cyber Security Incidents (R6.2), maintain logs of system events related to cybersecurity for these 11 Cyber Assets within the ESP (R6.3), retain all logs specified in R6 for 90 calendar days (R6.4), and review logs of system events related to cybersecurity (R6.5).

The Regions determined the duration of the violation to be from the date the Standard became mandatory and enforceable as to URE to when URE completed its Mitigation Plan.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other

system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

During SERC's Compliance Audit of URE2, SERC discovered a violation of CIP-007-3 R6. For one Cyber Asset within the ESP, URE2 failed to retain logs for 90 calendar days as required by CIP-007-3 R6.4. URE2 erased and rebuilt the server, and it produced logs for the other two of four sampled days.

The Regions determined the duration of the violation to be from the date the logs were missing to the date the Cyber Asset began producing logs.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

URE1 submitted a Self-Report to Reliability*First* identifying an additional instance of the violation of CIP-007-3 R6. URE1 replaced an email server, thereby changing the IP address for the email server. URE1, however, did not update the new IP address on the log aggregation server that issues alerts for detected Cyber Security Incidents. When URE1 removed the old email server the server was no longer issuing alerts to the correct email server. As a result, for one of its facilities, URE1 failed to ensure that the security monitoring controls issue automated or manual alerts for detected Cyber Security Incidents, as required by CIP-007-3 R6.2.

The Regions determined the duration of the violation to be from the date URE1 removed the old email server from service to the date URE1 reconfigured alerts to be sent to the appropriate email server.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3 R6 has the potential to affect the reliable operation of the BPS by providing the opportunity for undetected compromise of CCAs and other

system events that are related to cybersecurity to occur without the entity's knowledge. The risk to the BPS was mitigated by the following factors. The ESP at issue has an intrusion protection sensor that will block any suspicious traffic it senses trying to enter the ESP through the electronic access point. Operations personnel locally monitor operational status 24 hours a day, seven days a week, and if the system was compromised, URE would immediately disconnect the plant from the URE networks pursuant to its CIP-008 incident response plans. Network connection is not critical for this facility; URE can operate it locally. In addition to site physical security, all devices were located within a PSP. Furthermore, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

URE1 submitted a Self-Report to Reliability*First* identifying an additional instance of the violation of CIP-007-3 R6. For two Cyber Assets within the ESP, URE1 failed to submit a TFE because of the Cyber Assets' inability to support security status monitoring. URE1 implemented the compensating measures submitted in the TFE upon commissioning the Cyber Assets.

The Regions determined the duration of the violation to be from the date URE1 installed one of the devices through when URE1 submitted a TFE.

The Regions determined that this violation posed a minimal risk to the reliability of BPS, but did not pose a serious or substantial risk. Upon commissioning the Cyber Assets, URE1 implemented the following compensating measures. All devices reside within an ESP and PSP with alarming contacts back to the security console, which is monitored 24 hours a day, seven days a week. Only individuals who have been valid PRAs and cybersecurity training have access to these devices.

CIP-007-3a R8

CIP-007-3a R8 provides in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> ***
>
> R8.2 A review to verify that only ports and services required for operation of the Cyber Assets within the Electronic Security Perimeter are enabled;

***

R8.4 Documentation of the results of the assessment, the action plan to remediate or mitigate vulnerabilities identified in the assessment, and the execution status of that action plan.

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

URE1 self-certified non-compliance with CIP-007-3a R8 to Reliability*First*. URE2 submitted a Self-Report to SERC identifying a violation of CIP-007-3a R8. URE failed to perform a complete CVA for Cyber Assets within the ESP for the prior year. Specifically, URE failed to include 14 switches of its 300 Cyber Assets in Reliability*First* and 31 of its 700 Cyber Assets in SERC in the review to verify that only ports and services required for operation of the Cyber Assets are enabled, in violation of CIP-007-3a R8.2. In addition, URE failed to document the action plan to remediate or mitigate vulnerabilities identified in the assessment, as required by CIP-007-3a R8.4.

The Regions determined the duration of the violation to be from the date URE performed its incomplete CVA for the prior year to the date URE completed the CVA.

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-007-3a R8 has the potential to affect the reliable operation of the BPS by providing the opportunity for the system to be open to vulnerabilities that an entity has failed to identify. The risk to the BPS was mitigated by the following factors. Regarding the 14 switches URE failed to include in its ports and services review, as well as the 31 Cyber Assets, all firewall rules were in place. Furthermore, when URE completed the assessment it discovered no issues.

URE1 submitted a Self-Report to Reliability*First* identifying an additional violation of CIP-007-3a R8. URE1 commissioned three Cyber Assets within the ESP at one of its facilities. However, URE1 failed to include these three Cyber Assets in its cyber vulnerability assessment because the router configuration prevented the scanning tool from reaching these devices during the assessment.

The Regions determined the duration of the violation to be from the date URE1 commissioned these devices through the date URE performed the CVA.

The Regions determined that this violation posed a minimal risk to the reliability of BPS, but did not pose a serious or substantial risk. The three devices were not remotely accessible and they exist on a non-routable virtual LAN connected to a router within the ESP. In addition, when URE1 performed the CVA, it discovered no issues with the three devices.

CIP-008-3 R1

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

CIP-008-3 R1 provides in pertinent part:

> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan and implement the plan in response to Cyber Security Incidents. The Cyber Security Incident response plan shall address, at a minimum, the following:
>
> > R1.1 Procedures to characterize and classify events as reportable Cyber Security Incidents.

***

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

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-008-3 R1. URE2 submitted a Self-Report to SERC identifying a violation of CIP-008-3 R1. URE has in place a Cyber Security Incident response plan at the enterprise level that includes roles and responsibilities, response procedures, and contact information, but does not include processes or procedures to characterize or classify when a Cyber Security Incident is reportable, as required by CIP-008-3 R1.1.

The Regions determined that URE had a violation of CIP-008-3 R1 for failing to include procedures to characterize and classify events as reportable Cyber Security Incidents in its Cyber Security Incident response plan.

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

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-008-3 R1 has the potential to affect the reliable operation of the BPS by delaying an entity's ability to respond, resolve, and recover from a Cyber Security Incident. The risk to the reliability of the BPS was mitigated by the following factors. URE provides training regarding the availability of incident response plans during the cybersecurity training required for access to CCAs. Those individuals involved in the incident response process participate in annual drills that reinforce the initial training by discussing details of incident identification, classification, and reporting of incidents. In addition, URE experienced no Cyber Security Incidents during the time period of the violation. Furthermore, URE has several protections in place that reduce the risk to reliability of the BPS. In addition to site physical security, all devices were located within a PSP. Finally, URE protected and restricted remote access to the ESP using techniques such as limiting remote access to individuals who had two-factor authentication and were members of a restricted directory service group.

CIP-009-3 R5

The purpose statement of Reliability Standard CIP-009-3 provides: "Standard CIP-009-3 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-009-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-009-3 R5 provides: "Testing Backup Media — Information essential to recovery that is stored on backup media shall be tested at least annually to ensure that the information is available. Testing can be completed off site."

CIP-009-3 R5 has a "Lower" VRF and a "Severe" VSL.

During Reliability*First*'s Compliance Audit of URE1, Reliability*First* discovered a violation of CIP-009-3 R5. URE2 submitted a Self-Report to SERC identifying a violation of CIP-002-3 R2. Although two of URE's functions performed testing of backup media, the scope of the testing did not include testing to ensure that the information stored on backup media was available.

The Regions determined that URE had a violation of CIP-009-3 R5 for failing to test annually information essential to recovery that is stored on backup media to ensure that the information is available.

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

The Regions determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. Specifically, a violation of CIP-009-3 R5 has the potential to affect the reliable operation of the BPS by providing the opportunity for the prevention of or a delay in the entity's restoration of CCA. The risk to the BPS was mitigated by the fact that URE previously used a tape backup system and a software solution designed to back up systems automatically and regularly and store those backups for easy recovery. URE has in place redundant devices with real-time failover capability that it could use to replace, or fail operations over to, a device that needs restoration.

Regional Entities' Basis for Penalty

According to the Settlement Agreement, the Regions have assessed a penalty of three hundred fifty thousand dollars ($350,000) for the referenced violations. In reaching this determination, the Regions considered the following factors:

1. URE's compliance history was considered an aggravating factor;
2. URE self-reported several of the violations, as discussed herein, which the Regions considered a mitigating factor;[9]
3. URE did not promptly submit Mitigation Plans to remediate many of the violations, which the Regions considered as an aggravating factor;
4. URE was cooperative throughout the compliance enforcement process;
5. URE had an internal compliance program (ICP) at the time of the violations which the Regions considered a mitigating factor. However, due to evidence of URE's lack of effective internal controls, Reliability*First* only applied partial mitigating credit. Specifically, most of URE's violations appear to have been caused by URE's lack of execution and coordination of programs and procedures, especially across various business units;
6. the violation of CIP-002-3 R3 posed a serious and substantial risk to the reliability of the BPS and the other violations did not pose a serious or substantial risk to the reliability of the BPS, as described above;
7. there was no evidence of any attempt by URE to conceal the violations;

[9] The Regions did not apply mitigating credits for those Self-Reports that URE submitted immediately preceding and as a result of the Compliance Audits.

8. there was no evidence that URE violations were intentional;
9. URE committed to performing certain above and beyond actions; and
10. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, the Regions determined that, in this instance, the penalty amount of three hundred and fifty thousand dollars ($350,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[10]

CIP-002-3 (RFC2011001057)

URE's Mitigation Plan to address its violation of CIP-002-3 R3 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007405 and was submitted as non-public information to FERC in accordance with FERC orders. URE notified Reliability*First* that URE determined an additional mitigating action was necessary to achieve compliance with CIP-002-3 R3. Reliability*First* accepted URE1's proposed milestone addition.

URE's Mitigation Plan required URE to:

1. update CCA list using a manual process to supplement the automated process;
2. document the manual process to evaluate any asset that is not Windows or Linux-based;
3. implement the requirements of CIP-003 through CIP-009 for the CCAs; and
4. provide training to applicable personnel on asset commissioning.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

[10] *See* 18 C.F.R § 39.7(d)(7).

CIP-002-3 (RFC2012001319)

URE's Mitigation Plan to address its violation of CIP-002-3 R3 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007401 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify all CCAs based on a revised interpretation of the CCA methodology;
2. update the CCA list, review and update the CCA methodology to include an appropriate level of detail, and reapply the CCA methodology and update the CCA list as necessary; and
3. commit to implement the requirements of CIP-003 through CIP-009 for all CCAs.

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

As of the date of the filing, Reliability*First* has not verified completion of the Mitigation Plan for this violation.

CIP-002-3 (RFC2011001243)

URE's Mitigation Plan to address its violation of CIP-002-2 R3 was submitted to Reliability*First* stating it had been completed 2. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008263 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. include devices in CCA assessment and list and afford devices protective measures of CIP standards;
2. identify personnel that require training related to the violation; and
3. provide training to personnel.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-003-3 R4 (RFC2011001058)

URE's Mitigation Plan to address its violation of CIP-003-3 R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan to Reliability*First* stating URE would complete all mitigating actions. URE requested a Mitigation Plan completion extension which was granted by Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008131 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify project manager and project team;
2. review all current CCA information processes and procedures;
3. identify and document all CCA Information repositories;
4. identify who has access to the data at each step;
5. identify which authorities are granted to personnel with access; and
6. train personnel on changes to documentation, processes, and procedures.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-003-3 R5 (RFC2012010396)

URE's Mitigation Plan to address its violation of CIP-003-3 R5 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT009032-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. establish an overarching process document for performance of annual reviews of access privileges and the annual review of the program;
2. committed that each business unit/support group will:
    a. perform a gap analysis between current business unit/support group procedures and the overarching process to verify it meets the requirements and document those results;
    b. remediate any identified gaps by updating each respective procedure; and
    c. perform the review of access privileges to protected information.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-003-3 R6 (RFC2012009880)

URE's Mitigation Plan to address its violation of CIP-003-3 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007403 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review the process and procedure documentation to ensure it provides sufficient evidence of changes;
2. update change control documentation;
3. conduct training for all personnel involved; and
4. implement updated processes and procedures.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-004-3 R4 (RFC2011001244)

URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008264 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove access for affected employees;
2. review and update current procedures for granting and revoking NERC access at an enterprise level;
3. develop training for managers; and
4. conduct training for managers.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-004-3 R4 (RFC2011001264)

URE's Mitigation Plan to address its violation of CIP-004-3 R4 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan to Reliability*First*. URE2 submitted to SERC a Mitigation Plan to address the violations of CIP-004-3 R4, consolidated into RFCMIT008265-1. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008265-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove all affected access; and
2. review and update current procedures for granting and revoking NERC access at an enterprise level, and develop and conduct training for managers.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-005-3 R1 (RFC201100876)

URE's Mitigation Plan to address its violation of CIP-005-3 R1 was submitted to Reliability*First*. URE requested a Mitigation Plan completion extension which was granted by Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007838-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop and document new criteria to be used for the identification of EACMs;
2. complete a preliminary gap assessment to determine CIP compliance for the currently-identified EACMs to the ESP;
3. identify and document classification for all field and enterprise-wide EACMs using the newly-developed criteria;
4. develop an action plan to address areas of noncompliance for currently identified EACMs to the ESP;
5. complete the final gap assessment to identify any remaining areas of noncompliance for currently identified EACMs to the ESP; and
6. implement and complete the action plan to address all areas of noncompliance for currently identified EACMs to the ESP.

As of the date of the filing, URE has not certified and Reliability*First* has not verified completion of the Mitigation Plan for this violation.

CIP-005-3 R1 (RFC2012001318)

URE's Mitigation Plan to address its violation of CIP-005-3 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008268 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop and document new criteria to use for the identification of field and enterprise electronic access points;

2. use the newly-developed criteria to examine the classification criteria to identify where URE misinterpreted the Requirement to identify all electronic access points to the ESP; and
3. apply the classification criteria to identify the electronic access points to the ESP where URE misinterpreted the Requirement, and conduct refresher training for applicable personnel on the asset commissioning procedure.

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

As of the date of the filing, Reliability*First* has not verified completion of the Mitigation Plan for this violation.

CIP-005-3 R2 (RFC2012001317)

URE's Mitigation Plan to address its violation of CIP-005-3 R2 was submitted to Reliabiilty*First*. URE requested a Mitigation Plan completion extension which was granted by Reliability*First*. The Mitigation Plan was accepted by Reliabiilty*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007424 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. develop a plan for changes to disable any unnecessary ports and services;
2. review all firewalls rules and router configurations at electronic access points to identify all unnecessary ports and services;
3. develop and document new procedures for configuration of the ports and services; and
4. implement support configuration and procedures for control center, transmission, and generation groups to afford the protective measures specified in CIP-005 R2.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-005-3a R3 (RFC2012001316)

URE submitted to Reliability*First* a Mitigation Plan to address the violation of CIP-005-3a R3. URE's revised Mitigation Plan to address its violation of CIP-005-3a R3 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC.

The Mitigation Plan for this violation is designated as RFCMIT008267 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. install a second intrusion detection and prevention system device at this location to provide redundancy and ensure continuous monitoring and prevent recurrences; and
2. request rule changes necessary to allow sending of logs for the devices at issue.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-005-3a R4 (RFC201100877)

URE's Mitigation Plan to address its violation of CIP-005-3a R4 was submitted to Reliabiilty*First*. The Mitigation Plan was accepted by Reliabiilty*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007843 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. complete the full scans and compared the results against the original scan wherein URE determined that the known closed ports were closed; and
2. commit to enhance the CVA program to include:
    a. a review of all firewall rules for necessity regardless of whether it used them;
    b. identification of access points through a network walkdown, scans, wireless scans, and war dialing;
    c. development of a schedule to complete the scans and document remediation activities; and
    d. documentation of assessment deliverables.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-005-3 R5 (RFC2012010397)

URE's Mitigation Plan to address its violation of CIP-005-3 R5 was submitted to Reliabiilty*First* . The Mitigation Plan was accepted by Reliabiilty*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008999-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. create a slide to add to the pre-audit training materials emphasizing lessons learned and the importance of obtaining and delivering data to auditors in a timely manner; and
2. conduct a document review of the document it failed to annually review and update its scheduling system to set reminders for performing that review.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3 R1 (RFC201100878)

URE's Mitigation Plan to address its violation of CIP-006-3 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008128 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. close the openings in the six-wall border;
2. secure the PSP access point and provided the security awareness publication to the affected employees and their management;

3. issue disciplinary letters to the employees at issue;
4. review the existing physical security section of the cybersecurity training and identify and implement enhancements to the access control and visitor management procedures; and
5. update the physical security plan to include restricted key backup process information and an annual review of reference documents.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-006-3 R2 (RFC201100879)

URE submitted to Reliability*First* a Mitigation Plan to address the violation of CIP-006-3 R2. URE's revised Mitigation Plan to address its violation of CIP-006-3 R2 was submitted to Reliability*First*. URE requested a Mitigation Plan completion extension which was granted by Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008129-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify a project manager and project team, define the project scope and prepare a charter, complete a preliminary gap assessment to determine CIP compliance for currently-identified PACM devices, and develop an action plan to address areas of non-compliance for currently-identified PACM devices;
2. complete a final gap assessment to identify any remaining issues of non-compliance for currently-identified PACM devices;
3. complete the action plan to address all areas of non-compliance for currently-identified PACM device;
4. develop and document new criteria for the identification of other PACM devices;
5. identify and document classification for all other PACM devices, develop and finalize a strategy for other PACM devices related to dedicated and/or non-dedicated resources;
6. develop and document new configuration and procedures for other PACM devices;
7. develop a detailed implementation schedule for new configuration and procedures for all other PACM devices;
8. submit TFEs related to the physical access control system as applicable;

9. implement compliance processes and controls for the requisite Requirements; and
10. communicate or provide applicable training to requisite personnel.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-006-3 R4 (RFC201100880)

URE's Mitigation Plan to address its violation of CIP-006-3 R4 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007423 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. order new keys and cores, replace the lock cores;
2. recorded the names of individuals who received new keys;
3. establish standards and processes for the key program to document the trail of custody regarding CIP locks and keys; and
4. update its key control procedure.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3c R5 (RFC2012010022)

URE's Mitigation Plan to address its violation of CIP-006-3 R5 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008012 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to train all security console operators on the NERC CIP response procedure.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-006-3c R5 (RFC2013011723)

URE's Mitigation Plan to address its violation of CIP-006-3 R5 was submitted to Reliability*First* stating it was complete. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008950 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. perform a backout to the previous operating system to recover and fix the issue;
2. monitor the door once it discovered the issue; and
3. replace the defective processor board on the door and performed operational testing to confirm proper operation.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R1 (RFC2012009881)

URE submitted to Reliability*First* a Mitigation Plan to address the violation of CIP-007-3 R1. URE's revised Mitigation Plan to address its violation of CIP-007-3 R1 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007554 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. review its testing process and procedure to ensure it provides sufficient evidence of cybersecurity controls testing;

2. update test procedure documentation;
3. conduct training for all personnel involved in testing, and implement updated processes and procedures; and
4. provide training to applicable personnel regarding the procedures.

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

After reviewing URE's submitted evidence, Reliabiilty*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R2 (RFC2012001315)

URE's Mitigation Plan to address its violation of CIP-007-3 R2 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007963 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. disable all ports and services not required for normal and emergency operations;
2. review and enhance processes and procedures used to manage ports and services to provide clear direction for ports and services management expectations;
3. review and enhance the change control and testing process to increase the visibility of changes to ports and services and ensure that changes to ports and services are reviewed and either rejected or accepted;
4. apply enhanced processes and procedures to all CCAs and non-Critical Cyber Assets within the ESP; and
5. ensure that it generates complete baselines with justifications.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R3 (RFC2011001112)

URE's Mitigation Plan to address its violation of CIP-007-3 R3 was submitted to Reliability*First* o. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007404 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. developed and documented a program for monitoring all software-related security updates that includes both automated tools and manual processes; and
2. implemented both automated monitoring tools and manual processes and procedures to be informed of all security patches and updates.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R4 (RFC2011001060)

URE's Mitigation Plan to address its violation of CIP-007-3 R4 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007835 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to submit a TFE for the applicable devices.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R5 (RFC201100881)

URE's Mitigation Plan to address its violation of CIP-007-3 R5 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan to Reliability*First* with a proposed completion date of August 31,

2012. The Mitigation Plan was accepted by Reliability*First* on September 27, 2012 and approved by NERC on October 19, 2012. The Mitigation Plan for this violation is designated as RFCMIT008132 and was submitted as non-public information to FERC on October 19, 2012 in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. document a new password policy to specify the minimum password criteria required by CIP-007-3 R5.3;
2. file TFEs for 24 of the 26 devices discovered on October 1, 2010; and
3. file TFEs for devices impacted by CAN-0017.

URE certified on November 9, 2012 that the above Mitigation Plan requirements were completed on November 9, 2012.[11] URE submitted evidence of completion of its Mitigation Plan.

On March 7, 2013, after reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed on August 27, 2012.

CIP-007-3 R5 (RFC2011001062)

URE's Mitigation Plan to address its violation of CIP-007-3 R5 was submitted to Reliability*First* on February 29, 2012. URE submitted a revised Mitigation Plan to Reliability*First* on July 31, 2012 with a proposed completion date of August 31, 2012. The Mitigation Plan was accepted by Reliability*First* on September 27, 2012 and approved by NERC on October 19, 2012. The Mitigation Plan for this violation is designated as RFCMIT008133 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. document a new password policy to specify the minimum password criteria required by CIP-007-3 R5.3;
2. file TFEs for 24 of the 26 devices; and
3. file TFEs for devices impacted by CAN-0017.

[11] Although the Settlement Agreement at paragraph 338 states that URE certified completion of the Mitigation Plan on August 31, 2012, the correct date is November 9, 2012.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R5 (RFC2011001113)

URE's Mitigation Plan to address its violation of CIP-007-3 R5 was submitted to Reliability*First*. URE submitted a revised Mitigation Plan to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008134 and was submitted as non-public information to FERC in accordance with FERC orders. URE's Mitigation Plan required URE to:

1. document a new password policy to specify the minimum password criteria required by CIP-007-3 R5.3;
2. file TFEs for 24 of the 26 devices; and
3. file TFEs for devices impacted by CAN-0017.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R5 (RFC2012001314)

URE submitted to a Mitigation Plan to address its violation of CIP-007-3 R5. URE submitted a revised Mitigation Plan to address its violation of CIP-007-3 R5 to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007486 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. identify its systems with shared accounts;
2. verify that the passwords have been changed within the past year;

3. verify that each system with shared accounts has a logging mechanism to provide audit trail evidence;
4. implement processes to provide audit trail evidence as necessary,
5. implement a TFE checklist to assess assets for TFEs prior to placing them into production; and
6. conduct training for appropriate personnel in the execution of these processes.

As of the date of the filing, URE has not certified and Reliability*First* has not verified completion of the Mitigation Plan for this violation.

CIP-007-3 R6 (RFC201100882 and RFC2011001064)

URE's Mitigation Plan to address its violation of CIP-007-3 R6 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007402 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. remove the printer from the ESP; and
2. submit a TFE for the applicable device.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-007-3 R6 (RFC2011001114)

URE's Mitigation Plan to address its violation of CIP-007-3 R6 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007836 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. ensure the monitoring tool captures log data;

2. verify logging targets in scope;
3. identify technical logging abilities and limitations;
4. create a process for determining whether log monitoring is interrupted or data is not being collected;
5. committed to fix the firewall rule to allow for alerts to be sent to appropriate personnel;
6. implement a heartbeat alert so the log aggregator tool will send a daily "dummy" alert to indicate that it is functioning;
7. implement a new firewall rule change process for the firewalls to ensure adequate communication of changes to appropriate personnel; and
8. submit a TFE and send an email communication to notify relevant personnel of the importance of submitting a TFE prior to commissioning or installing a new asset and using a TFE checklist.

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

As of the date of the filing, Reliability*First* has not verified completion of the Mitigation Plan for this violation.

CIP-007-3a R8 (RFC2011001245)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was submitted to Reliability*First* o stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007406 and was submitted as non-public information to FERC in accordance with FERC orders. When preparing its certification of completion for this Mitigation Plan, URE discovered that it failed to complete the mitigating activities as stated in the Mitigation Plan and prevented future reoccurrence of the violation. URE submitted additional mitigating activities.

URE's Mitigation Plan required URE to:

1. complete a CVA ; and
2. remove the devices from the ESP by reconfiguring the router.

The additional mitigating activities URE submitted required URE to:

3. develop a project plan to remove these devices from the ESP by reconfiguring the router as a documented electronic Access Point; and
4. implement the project plan during an appropriate unit outage window.

The Mitigation Plan is scheduled to be completed at a later date.

CIP-007-3a R8 (RFC201100883)

URE's Mitigation Plan to address its violation of CIP-007-3a R8 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT007839 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Complete the CVAs and enhance the CVA program to include:
    a. creation of a statement of work between the departments involved that defines the scope of the scans, access management, and scanning methodology;
    b. develop a schedule to complete the scans and document remediation activities; and
    c. clearly document assessment deliverables.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-008-3 R1 (RFC2012010398)

URE's Mitigation Plan to address its violation of CIP-008-3 R1 was submitted to Reliability*First* stating it had been completed. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008719 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to revise its Cyber Security Incident response plan to include:

1. examples of triggers;
2. steps for determining whether any NERC CCAs are impacted; and
3. steps for determining whether reporting to the ES-ISAC is required.

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

After reviewing URE's submitted evidence, Reliability*First* verified that URE's Mitigation Plan was completed.

CIP-009-3 R5 (RFC2012010400)

URE's Mitigation Plan to address its violation of CIP-009-3 R5 was submitted to Reliability*First*. The Mitigation Plan was accepted by Reliability*First* and approved by NERC. The Mitigation Plan for this violation is designated as RFCMIT008557 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to include detailed testing procedures for all asset types including non-computer devices in its procedures and conducting those tests.

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

As of the date of the filing, Reliability*First* has not verified completion of the Mitigation Plan for this violation.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[12]

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,[13] the

[12] *See* 18 C.F.R. § 39.7(d)(4).

[13] *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).

NERC BOTCC reviewed the Settlement Agreement and supporting documentation on July 9, 2013. The NERC BOTCC approved the Settlement Agreement, including the Regions' assessment of a three hundred fifty thousand dollar ($350,000) 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 Regions considered URE's compliance history as an aggravating factor in penalty determination, as discussed above;
2. URE self-reported some of the violations;
3. URE did not promptly submit Mitigation Plans to remediate many of the violations, which the Regions considered as an aggravating factor;
4. Reliability*First* reported that URE was cooperative throughout the compliance enforcement process;
5. URE had a compliance program at the time of the violation which the Regions considered a mitigating factor, as discussed above;
6. The Regions determined that the CIP-002-3 R3 violation posed a serious and substantial risk to the reliability of the BPS and the other violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. there was no evidence that URE violations were intentional;
9. URE committed to performing certain above and beyond actions, as discussed above; and
10. The Regions 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 three hundred and fifty thousand dollars ($350,000) 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 the Regions and URE, included as Attachment a;

b) Record documents for the violation of CIP-002-3 R3, included as Attachment b:

   1. URE's Self-Report;
   2. URE's Self-Report;
   3. URE's Self-Report;
   4. URE's Self-Report;
   5. SERC Compliance Audit document;
   6. URE's Self-Report;

7. URE's Self-Report;
8. URE's Mitigation Plan designated as RFCMIT007405;
9. URE's Mitigation Plan designated as RFCMIT007401;
10. URE's Mitigation Plan designated as RFCMIT008263;
11. URE's Certification of Mitigation Plan Completion for RFCMIT007405;
12. URE's Certification of Mitigation Plan Completion for RFCMIT008263;
13. URE's Certification of Mitigation Plan Completion for RFCMIT007401;
14. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT008263;
15. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT007405;

c) Record documents for the violation of CIP-003-3 R4, included as Attachment c:
   1. URE's Self-Report;
   2. URE's Mitigation Plan designated as RFCMIT008131;
   3. URE's Certification of Mitigation Plan Completion;
   4. Reliability*First*'s Verification of Mitigation Plan Completion;

d) Record documents for the violation of CIP-003-3 R5, included as Attachment d:
   1. URE's Self-Report;
   2. Reliability*First*'s Summary of Possible Violation;
   3. Reliability*First*'s Summary of Possible Violation;
   4. URE's Mitigation Plan designated as RFCMIT009032-1;

e) Record documents for the violation of CIP-003-3 R6, included as Attachment e:
   1. SERC Compliance Audit document;
   2. URE's Self-Report;
   3. Reliability*First*'s Summary of Possible Violation;
   4. URE's Self-Report;
   5. URE's Mitigation Plan designated as RFCMIT007403;
   6. URE's Certification of Mitigation Plan Completion;

7. Reliability*First*'s Verification of Mitigation Plan Completion;

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

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. ReliabilityFirst's Summary of Possible Violation document;
7. URE's Self-Report;
8. URE's Mitigation Plan designated as RFCMIT008264;
9. URE's Mitigation Plan designated as RFCMIT008265-1;
10. URE's Certification of Mitigation Plan Completion for RFCMIT008264;
11. URE's Verification of Mitigation Plan Completion for RFCMIT008264;

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

1. SERC Compliance Audit document;
2. URE's Self-Report;
3. Reliability*First*'s Summary of Possible Violation;
4. URE's Self-Certification;
5. URE's Self-Report;
6. URE's Mitigation Plan designated as RFCMIT007838-1;
7. URE's Mitigation Plan designated as RFCMIT008268;
8. URE's Certification of Mitigation Plan Completion for RFCMIT008268;

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

1. SERC Compliance Audit document;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT007424;

i) Record documents for the violation of CIP-005-3a R3, included as Attachment i:

1. URE's Self-Report;
2. Reliability*First*'s Summary of Possible Violation;
3. URE's Mitigation Plan designated as RFCMIT008267;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

j) Record documents for the violation of CIP-005-3a R4, included as Attachment j:

1. URE's Self-Certification;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Mitigation Plan designated as RFCMIT007843;
5. URE's Certification of Mitigation Plan Completion;
6. Reliability*First*'s Verification of Mitigation Plan Completion;

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

1. Reliability*First*'s Summary of Possible Violation;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT008999;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

l) Record documents for the violation of CIP-006-3 R1, included as Attachment l:

1. URE's Self-Certification;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. Reliability*First*'s Summary of Possible Violation;

7. URE's Self-Report;
8. URE's Self-Report;
9. URE's Self-Report;
10. URE's Mitigation Plan designated as RFCMIT008128;

m) Record documents for the violation of CIP-006-3 R2, included as Attachment m:

1. URE's Self-Certification;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT008129;

n) Record documents for the violation of CIP-006-3 R4, included as Attachment n:

1. URE's Self-Certification;
2. URE's Mitigation Plan designated as RFCMIT007423;
3. URE's Certification of Mitigation Plan Completion;
4. Reliability*First*'s Verification of Mitigation Plan Completion;

o) Record documents for the violation of CIP-006-3c R5, included as Attachment o:

1. URE's Self-Report;
2. URE's Self-Report;
3. Reliability*First*'s Summary of Possible Violation;
4. URE's Mitigation Plan designated as RFCMIT008012;
5. URE's Mitigation Plan designated as RFCMIT008950;
6. URE's Certification of Mitigation Plan Completion for RFCMIT008012;
7. URE's Certification of Mitigation Plan Completion for RFCMIT008950;
8. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT008012;
9. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT008950;

p) Record documents for the violation of CIP-007-3 R1, included as Attachment p:

1. SERC Compliance Audit document;
2. URE's Self-Report;

3. URE Self-Report;
4. URE's Self-Report;
5. URE's Mitigation Plan designated as RFCMIT007554;
6. URE's Certification of Mitigation Plan Completion;
7. Reliability*First*'s Verification of Mitigation Plan Completion;

q) Record documents for the violation of CIP-007-3 R2, included as Attachment q:

1. SERC Compliance Audit document;
2. URE's Self-Report;
3. Reliability*First*'s Summary of Possible Violation;
4. URE's Mitigation Plan designated as RFCMIT007963;
5. URE's Certification of Mitigation Plan Completion;
6. Reliability*First*'s Verification of Mitigation Plan Completion;

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

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT007963;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

s) Record documents for the violation of CIP-007-3 R4, included as Attachment s:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Mitigation Plan designated as RFCMIT007835;
5. URE's Certification of Mitigation Plan Completion;
6. Reliability*First*'s Verification of Mitigation Plan Completion;

t) Record documents for the violation of CIP-007-3 R5, included as Attachment t:

1. URE's Self-Certification;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. SERC Compliance Audit document;
7. URE's Self-Report;
8. URE's Self-Report;
9. Reliability*First*'s Summary of Possible Violation;
10. URE's Mitigation Plan designated as RFCMIT008132;
11. URE's Mitigation Plan designated as RFCMIT008133;
12. URE's Mitigation Plan designated as RFCMIT008134;
13. URE's Mitigation Plan designated as RFCMIT007486;
14. URE's Certification of Mitigation Plan Completion for RFCMIT008132;
15. URE's Certification of Mitigation Plan Completion for RFCMIT008133;
16. URE's Certification of Mitigation Plan Completion for RFCMIT008134;
17. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT008132, RFCMIT008133, and RFCMIT008134;

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

1. URE's Self-Report;
2. URE's Self-Certification;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. SERC Compliance Audit document;
7. URE's Self-Report;

8. URE's Self-Report;
9. URE's Mitigation Plan designated as RFCMIT007402;
10. URE's Mitigation Plan designated as RFCMIT007836;
11. URE's Certification of Mitigation Plan Completion for RFCMIT007402;
12. URE's Certification of Mitigation Plan Completion for RFCMIT007836;
13. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT007402;

v) Record documents for the violation of CIP-007-3a R8, included as Attachment v:

1. URE's Self-Certification;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Mitigation Plan designated as RFCMIT007406;
5. URE's Mitigation Plan designated as RFCMIT0078392;
6. URE's Certification of Mitigation Plan Completion for RFCMIT007839;
7. Reliability*First*'s Verification of Mitigation Plan Completion for RFCMIT007839;

w) Record documents for the violation of CIP-008-3 R1, included as Attachment w:

1. Reliability*First*'s Summary of Possible Violation;
2. URE's Self-Report dated;
3. URE's Mitigation Plan designated as RFCMIT008719;
4. URE's Certification of Mitigation Plan Completion;
5. Reliability*First*'s Verification of Mitigation Plan Completion;

x) Record documents for the violation of CIP-009-3 R5, included as Attachment x:

1. Reliability*First*'s Summary of Possible Violation;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as RFCMIT008557; and
4. URE's Certification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[14]

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

[14] *See* 18 C.F.R § 39.7(d)(6).

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net 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 Marisa A. Sifontes* General Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org	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 Robert K. Wargo* Director of Analytics & Enforcement Reliability*First* Corporation 320 Springside Drive, Suite 300 Akron, OH 44333 (330) 456-2488 bob.wargo@rfirst.org

L. Jason Blake*
General Counsel
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
jason.blake@rfirst.org

Nicole D. Schaefer*
Managing Enforcement Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
niki.schaefer@rfirst.org

Megan E. Gambrel*
Attorney
Reliability*First* Corporation
320 Springside Drive, Suite 300
Akron, OH 44333
(330) 456-2488
megan.gambrel@rfirst.org

Maggie A. Sallah*
Senior Counsel
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 494-7778
(704) 357-7914 – facsimile
msallah@serc1.org

Andrea B. Koch*
Manager, Compliance Enforcement and Mitigation
SERC Reliability Corporation
2815 Coliseum Centre Drive, Suite 500
Charlotte, NC 28217
(704) 940-8219
(704) 357-7914 – facsimile
akoch@serc1.org

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

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: Unidentified Registered Entity 1 and Unidentified Registered Entity 2
ReliabilityFirst Corporation

Attachments