December 31, 2012

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP13-_-000

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because SERC and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of the violations[3] of CIP-002-1 Requirement (R)2 and R3, CIP-003-1 R1, CIP-004-1 R2 and R4, CIP-005-1 R1, R2, R3 and R4, CIP-006-1 R1, R3, R4, R5 and R6, CIP-007-1 R1, R2, R3, R4, R5, R6, R7 and R8, CIP-007-2a R6 and CIP-009-1 R1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of nine hundred fifty thousand dollars ($950,000), 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 SERC200900320,

[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.

SERC200900297, SERC201000515, SERC200900321, SERC200900283, SERC200900290, SERC201000480, SERC200900421, SERC201000483, SERC200900357, SERC200900393, SERC201000627, SERC201000486, SERC201000484, SERC200900310, SERC200900312, SERC200900313, SERC201000688, SERC200900315, SERC200900314, SERC201000577, SERC201000485, SERC201000479 and SERC200900316 are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement executed on December 20, 2012, by and between SERC and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
SERC Reliability Corporation	URE	NOC-1531	SERC200900320	CIP-002-1	R2	High[4]	$950,000
			SERC200900297	CIP-002-1	R3	Lower	
			SERC201000515	CIP-003-1	R1.2	Lower	
			SERC200900321	CIP-004-1	R2	Medium	
			SERC200900283	CIP-004-1	R4	Lower	
			SERC200900290	CIP-005-1	R1	Medium	

[4] When NERC filed Violation Risk Factors (VRFs) it originally assigned CIP-002-1 R2 a "Lower" VRF. The Commission approved the VRF as filed; however, it directed NERC to submit modifications. NERC submitted the modified "High" VRF and on January 27, 2009, the Commission approved the modified "High" VRF. Therefore, the "Lower" VRF for CIP-002-1 R2 was in effect from June 18, 2007 until January 27, 2009 when the "High" VRF became effective.

			SERC201000480	CIP-005-1	R2	Medium	
			SERC200900421	CIP-005-1	R3	Medium	
			SERC201000483	CIP-005-1	R4	Medium	
			SERC200900357	CIP-006-1	R1	Medium	
			SERC200900393	CIP-006-1	R3	Lower	
			SERC201000627	CIP-006-1	R4	Medium	
			SERC201000486	CIP-006-1	R5	Lower	
			SERC201000484	CIP-006-1	R6	Medium	
			SERC200900310	CIP-007-1	R1	Medium	
			SERC200900312	CIP-007-1	R2	Medium	
			SERC200900313	CIP-007-1	R3	Lower	
			SERC201000688	CIP-007-1	R4	Medium	
			SERC200900315	CIP-007-1	R5	Lower	
			SERC200900314	CIP-007-1	R6	Lower	
			SERC201000577	CIP-007-2a	R6	Lower	
			SERC201000485	CIP-007-1	R7	Lower	
			SERC201000479	CIP-007-1	R8	Lower	
			SERC200900316	CIP-009-1	R1	Medium	

SERC200900320 CIP-002-1 R2

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

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

CIP-002-1 R2 provides: "Critical Asset Identification — The Responsible Entity[5] shall develop a list of its identified Critical Assets determined through an annual application of the risk-based assessment methodology required in R1. The Responsible Entity shall review this list at least annually, and update it as necessary."

CIP-002-1 R2 has a "High" Violation Risk Factor (VRF) and a "High" Violation Severity Level (VSL). SERC sent URE a CIP Spot Check Notice referencing a scheduled Spot Check.

The SERC CIP Spot Check team reported a violation of CIP-002-1 R3 because URE failed to associate Critical Cyber Assets (CCAs) with Critical Assets. During the assessment, SERC determined this was actually a violation of CIP-002-1 R2, not R3, because URE did not include control centers in its annual Critical Asset list even though they were included in the annual CCA list. SERC determined that URE was in violation of CIP-002-1 R2 for failing to develop a complete list of Critical Assets by its compliance date.

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

SERC determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS) because the failure to identify Critical Assets and CCAs appropriately can lead to inadequate protection of CCAs. The violation did not pose a serious or substantial risk to the reliability of the BPS

[5] Within the text of Standards 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.

because the control system CCAs were on the annual CCA list and were being protected per the CIP Standards even though control centers were not on the annual Critical Asset list.

SERC200900297 CIP-002-1 R3

CIP-002-1 R3 provides:

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

CIP-002-1 R3 has a "Lower" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of CIP-002 R3. Each incident is numbered and discussed separately below:

1. URE self-reported that during a reconciliation of Cyber Assets within the Electronic Security Perimeter (ESP), it identified eight control center workstations that were CCAs that had been omitted from the CCA List. According to URE, the CCA list was developed from a manual compilation of URE's physical asset inventory. When a reconciliation of the physical asset inventory was made against a list of Cyber Assets that were identified by an automated reporting tool, omissions in the CCA list were found. SERC determined that URE failed to develop a complete list of CCAs.

2. While further analyzing the first Self-Report, URE discovered four switch devices that had not been included on the CCA List. URE submitted an addendum to the first Self-Report. After further examination, SERC learned that the switches were not included in URE's database, which is the source of URE's CCA list. Because of this, the CCA list was incomplete. SERC determined that URE failed to develop a complete list of CCAs.
3. URE self-reported that it had incorrectly listed an entire system as a single asset on its CCA list instead of the system's subcomponents. After further examination, SERC learned that the subcomponents were terminal servers that comprised URE's supervisory control and data acquisition (SCADA) Management Platform. Instead of listing each terminal server as a CCA, URE listed the SCADA Management Platform as a single CCA. Without listing the individual subcomponents as CCAs, it was impossible for URE to apply the other associated CIP Standards. SERC determined that URE failed to develop a complete list of CCAs.
4. As a result of its annual Cyber Vulnerability Assessment (CVA), URE self-reported a Cyber Asset that was not listed on its CCA List. After further examination, SERC learned that the communication processor was not included in URE's database, which is the source of URE's CCA list. Because of this omission, the CCA list was incomplete. SERC determined that URE failed to develop a complete list of CCAs.
5. URE self-reported 16 CCAs that had been documented as non-critical Cyber Assets. According to URE, the misclassification was found during an internal assessment of Cyber Assets within an ESP. After further examination, SERC learned that the 16 misclassified Cyber Assets were servers and energy management system (EMS) servers. SERC determined that URE failed to develop a complete list of CCAs.

SERC determined that URE was in violation of CIP-002 R3 because it failed to develop a complete list of CCAs for three years.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE's failure to develop a complete list of CCAs could have resulted in CCAs not being

afforded all of the protective measures of the CIP Standards. Without these protective measures the CCAs were at a greater risk of being compromised and rendered inoperable.

SERC201000515 CIP-003-1 R1

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

CIP-003-1 R1 provides, in pertinent part:

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

CIP-003-1 R1 has a "Medium" VRF; R1.1, R1.2 and R1.3 each have a "Lower" VRF.

This violation addresses two occurrences of CIP-003 R1.2. Each incident is discussed separately below:

1. SERC sent URE a CIP Spot Check Notice. The SERC CIP Spot Check team found that URE had not made its cyber security policy readily available to all persons who have access to, or are responsible for, CCAs, as required by CIP-003 R1.2. SERC learned that URE's cyber security policy was only available through its portal and could not be accessed without an URE Logon ID, which meant that 160 personnel with access to CCAs did not have access to the cyber security policy. SERC determined that URE failed to make its cyber security policy readily available to all persons who have access to, or are responsible for, CCAs.

2. While analyzing the incident found during the CIP Spot Check, URE found another instance of non-compliance under another segment of URE's operations. URE self-reported the finding. After further examination, SERC learned that URE's Cyber Security Policy for that segment was only available on the portal associated with such segment and could not be accessed without an URE Logon ID, which meant that three personnel with access to CCAs did not have access to the cyber security policy. SERC determined that URE failed to make its cyber security policy readily available to all persons who have access to, or are responsible for, CCAs.

SERC determined that URE was in violation of CIP-003-1 R1.2 because it failed to make its cyber security policy readily available to all personnel who have access to, or are responsible, for CCAs.

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

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Fewer than 12% of all personnel that had access to CCAs were unable to access URE's cyber security policy due to lack of an URE Logon ID. In addition, all personnel that had access to CCAs had received CIP-004 R2 Cyber Security Training. The CIP-004 R4 Cyber Security Training covered policies, use, and handling of CCAs as appropriate for particular roles and responsibilities.

SERC200900321 CIP-004-1 R2.1

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

CIP-004-1 R2 provides in pertinent part:

> R2. Training — The Responsible Entity shall establish, maintain, and document an annual cyber security training program for personnel having authorized cyber or authorized

unescorted physical access to Critical Cyber Assets, and review the program annually and update as necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained within ninety calendar days of such authorization.

CIP-004-1 R2 has a "Lower" VRF; R2.1 has a "Medium" VRF. SERC applied a "Severe" VSL.

SERC sent URE a CIP Spot Check Notice.

The SERC CIP Spot Check team identified a violation of CIP-004-1 R2.1. Three employees, who had access to CCAs, had not completed Cyber Security training within 90 days of receiving authorization access.

SERC learned that 7.0% of individuals, who had access to URE's CCAs, had not completed Cyber Security training within 90 days of receiving access authorization. URE explained that the individuals were not trained on time due to severe weather that prevented some personnel, contractors, and vendors from completing training, as they were either evacuated or working on storm restoration.

SERC determined the duration of the violation to be from 90 days after the Standard became mandatory and enforceable for URE through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because only 7% of the individuals who were granted access to CCAs received their initial Cyber Security training outside of the 90-day deadline. All of the individuals had personnel risk assessments (PRAs). All of the individuals eventually were trained or had their access revoked.

SERC200900283 CIP-004-1 R4

CIP-004-1 R4 provides:

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

CIP-004-1 R4 each have a "Lower" VRF. SERC applied a "Severe" VSL.

This violation addresses multiple occurrences of CIP-004 R4. Each incident is numbered and discussed separately below.

1. URE self-reported that two individuals who left the company under routine circumstances were not removed from the physical access list within seven days, as required by the Standard. SERC learned that one of the individuals was an intern. At that time, the intern's physical access keycard was collected but the intern was not removed from the access list until about two weeks after his or her last day. The second individual was an employee that retired. The employee's physical access keycard was collected at that time, but the employee was not removed from the access list until about a month later. SERC determined that URE failed to remove individuals that no longer required access to CCA from the physical access list within seven calendar days.
2. URE self-reported that at the time of another intern's last day the intern's physical access card was collected, but the intern was not removed from the physical access list until about a month

and half later. SERC determined that URE failed to remove an individual, who no longer required physical access to CCAs, from the physical access list within seven calendar days.

3. URE self-reported that a part-time employee resigned. The employee's physical access card was collected at that time, but the employee was not removed from the physical access list until about a month later. SERC determined that URE failed to remove an individual, who no longer required physical access to CCAs, from the physical access list within seven calendar days.
4. URE self-reported that a contractor, who retired, was not removed from the physical access list until about two months later. The contractor's physical access keycard was collected on the day of his retirement. SERC determined that URE failed to remove an individual that no longer required physical access to CCAs from the physical access list within seven calendar days.
5. URE self-reported that another contractor, who retired, did not have his read-only electronic access removed until eight days later. The contractor was removed from the physical access list, and his physical access keycard was collected on the day of his retirement. SERC determined that URE failed to remove an individual that no longer required electronic access to CCAs from the electronic access list within seven calendar days.
6. URE self-reported the discovery of an URE employee who transferred to a position that no longer required electronic access to CCAs. The employee's electronic access to CCAs was not removed until ten days later.

SERC determined that URE was in violation of CIP-004-1 R4 because it failed to update the access lists within seven calendar days of a change of personnel and to revoke access to CCAs within seven calendar days for personnel that no longer require access.

SERC determined the duration of the violation to be from the date of the initial violation through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because all of the personnel involved had the required CIP training and PRAs. All personnel involved were in good standing with URE, and none required access revocation because of termination. Because each individual's physical keycard had been confiscated, unescorted

physical access to CCAs would only have been granted if the individual provided a business need and had been authorized by the site's physical access approver. Finally, electronic access was missed by one day for the contractor that had read-only access and two days for the employee that was transferred to another position within URE.

SERC200900290 CIP-005-1 R1

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

CIP-005-1 R1 provides:

> R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).
>
> > R1.1. Access points to the Electronic Security Perimeter(s) shall include any externally connected communication end point (for example, dial-up modems) terminating at any device within the Electronic Security Perimeter(s).
> >
> > R1.2. For a dial-up accessible Critical Cyber Asset that uses a non-routable protocol, the Responsible Entity shall define an Electronic Security Perimeter for that single access point at the dial-up device.
> >
> > R1.3. Communication links connecting discrete Electronic Security Perimeters shall not be considered part of the Electronic Security Perimeter. However, end points of these communication links within the Electronic Security Perimeter(s) shall be considered access points to the Electronic Security Perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

R1.5. Cyber Assets used in the access control and monitoring of the Electronic Security Perimeter(s) shall be afforded the protective measures as a specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirements R2 and R3, Standard CIP-007, Requirements R1 and R3 through R9, Standard CIP-008, and Standard CIP-009.
R1.6. The Responsible Entity shall maintain documentation of Electronic Security Perimeter(s), all interconnected Critical and non-critical Cyber Assets within the Electronic Security Perimeter(s), all electronic access points to the Electronic Security Perimeter(s) and the Cyber Assets deployed for the access control and monitoring of these access points.

CIP-005-1 R1, R1.1, R1.2, R1.3, R1.4 and R1.5 each have a "Medium" VRF; R1.6 has a "Lower" VRF. SERC applied a "Severe" VSL.

This violation addresses multiple occurrences of CIP-005 R1. Each incident is numbered and discussed separately.

1. URE self-reported a violation of CIP-005-1 R1. According to URE, it failed to ensure that every CCA resided within an ESP by the compliance date for URE. The Self-Report indicated that URE failed to meet this Requirement for 23.8% of its sites containing CCAs. As of the compliance date for URE, URE had 76.2% of ESPs fully in place at its CCA sites. The remaining 23.8% of its sites had the necessary infrastructure in place for the ESPs; however, the ESPs could not be brought online because URE's primary EMS firewall management server, which is not directly related to establishing the ESPs, had failed. This caused a total communications outage at a major URE data center. URE stated that the affected data center was essential for the reliable operation of its EMS and a resolution was necessary before work could continue on establishing the ESPs. The data center was recovered, and URE established the 23.8% of the remaining ESPs. SERC determined that URE's ESPs were not established by the compliance date for URE.

2. During a manual network scan, URE discovered 82 Cyber Assets that had not been properly identified as access points to an ESP. URE performed the scan after identifying Cyber Assets within an ESP that did not have security status monitoring implemented as required by CIP-007-1 R6. The same day as the discovery, URE submitted an addendum to its self-report explaining that the control access devices had not been designated in its database as access points by the compliance date for URE. URE's database is used to document all critical and non-critical Cyber Assets and access points to the ESPs pursuant to CIP-005-1 R1.6. After further examination, SERC determined that URE failed to designate the console access devices as access points to the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points, CCAs, and Cyber Assets.

3. During the implementation of an improved network-scanning tool, URE identified 16 undocumented access points located within an ESP. URE submitted an addendum to its self-report detailing this incident. After further examination, SERC determined that URE failed to identify the access points within the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

4. After a departmental meeting discussing the importance of Cyber Asset identification, an employee reported an asset that was connected within an ESP was not documented. URE submitted an addendum to its self-report detailing this incident. The undocumented asset is used to remotely troubleshoot Remote Terminal Unit (RTU) circuits. URE personnel determined that the asset had been connected within an ESP since prior to the compliance date for URE. After further examination, SERC verified URE's use of the asset and determined that it failed to identify it as access points within the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

5. During a CIP Spot Check, the SERC Spot Check Team found that URE failed to document six printers as non-critical Cyber Assets within an ESP. URE explained that these printers had been identified during a previous network scan; however, URE mistakenly believed that the printers had already been documented. Upon receipt of the Spot Check Team's finding, SERC reviewed the evidence and discovered that URE had no procedures in place to reconcile what was found during the network scan with the devices in the database. SERC determined that URE failed to identify the printers as non-critical Cyber Assets within the applicable ESP due to insufficient

processes and procedures for the identification and documentation of ESP non-critical Cyber Assets.

6. URE submitted an addendum to its self-report detailing three undocumented access points into an ESP that were discovered. The first undocumented access point discovered was a printer located at URE's operation center. The printer had a dual network interface card (NIC) that was enabled, which opened an undocumented access point to the ESP. After further review, URE identified two more printers with the same configuration; one was located at the same operation center and the second was located at another operation center. According to URE, the printers were installed before the CIP Standards became enforceable. After further examination, SERC verified that URE was aware that the printers had a dual NIC configuration, but did not know that the printers needed to be documented when located in an ESP. SERC determined that URE failed to identify the printers as access point within the applicable ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

7. URE submitted an addendum to its self-report after it discovered incorrect ESP drawings for two substations. After further examination, SERC verified that the drawings had not been reviewed internally, nor had an on-site walk down been performed in order to assure the accuracy of the drawings. SERC determined that URE failed to correctly document the ESPs due to insufficient processes and procedures for maintaining and verifying ESP documentation.

8. While analyzing the incident from the addendum (discussed in item four), URE identified an undocumented server component located within an ESP. URE submitted an addendum to its self-report detailing this incident. The undocumented server component is located on a private network, which was not detectable by URE's previous scanning tool. According to URE, the person performing the server installation was unaware that components should be documented as access points. In addition, URE did not have its database in place at that time, which should have aided in the identification of the server components. SERC determined that URE failed to identify the server component as access points within the applicable ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

9. While analyzing the incident from the addendum (discussed in item 6), URE identified two servers with undocumented components located within an ESP. URE submitted an addendum

to its self-report. Each server had dual NIC cards that were connected to an ESP and a non-ESP network that had not been documented as access points. According to URE, the NICs were installed before the CIP Standards became enforceable. After further examination, SERC verified that URE knew the servers had a dual NIC configuration, but did not know that the servers needed to be documented when located in an ESP. SERC determined that URE failed to identify the NIC cards as access points within the applicable ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

10. URE self-reported multiple issues associated with documentation of assets within an ESP that were identified after performing the required annual CVA:

    a. Four servers with dual network connections had a network connection outside an ESP. This resulted in undocumented access points to the ESP. SERC determined that URE failed to identify the network connections as access points within the applicable ESP due to insufficient processes and procedures for the identification and documentation of ESP access points;

    b. Several documentation errors in the database were also identified:

        i. Incorrect serial numbers and device names for ESP assets;

        ii. Some Cyber Assets were incorrectly documented as being in an ESP; and

        iii. The location of a server at one of URE's operations center was incorrect.

        After further examination, SERC learned that the information came from the initial inventory that existed prior to the development of the many different spreadsheets and sources. According to URE, at the time the database was being developed, it had no inventory control, no physical inventory, and no control mechanisms to ensure the inventory remained accurate in a rapidly changing environment. As such, the data incorporated into the database was not verified; and

    c. An error regarding a network switch on the ESP diagram for a data center was also identified. After further examination, SERC verified that the labeling error occurred when the initial drawing was created. Further review by URE did not identify any similar labeling errors on ESP drawings.

11. URE self-reported six undocumented Cyber Assets that were discovered as a result of its CVA. The Cyber Assets were physically but not logically connected with an ESP. According to URE, each device's physical connection to the network was removed as part of follow-up CVA actions. After further examination, SERC verified that because these assets were not configured to communicate on the network, previous inventory scans failed to recognize them. They were identified when URE physically traced the ESP cabling. SERC determined that URE failed to identify the Cyber Assets within the applicable ESP due to insufficient processes and procedures for the identification and documentation of ESP Cyber Assets.

12. URE self-reported undocumented access points that were discovered as a result of its CVA:

    a. The firewalls were at a certain operations centers. According to URE, the appliance associated with the firewalls came with default community strings. The responsible personnel were supposed to change the default community strings to a secure community string when the firewalls were installed or the appliances were upgraded; however the change did not occur when an appliance upgrade was done at one operations center. After further examination, SERC learned that the issue was not detected during the pre-CIP compliance reviews performed prior to the mandatory and enforceable date for URE. Thus, the firewalls operated with the default setting potentially allowing unsecure read-only access to the ESP. When an appliance upgrade was performed at the operations center, URE did not have a firewall build procedure; thus, resources overlooked the community strings settings. With regard to the firewalls at other operations centers, they had a protocol disabled, which prevented the enabled community strings from being used to communicate outside the ESP. Because the firewalls could not communicate outside the ESP, they are not undocumented access points; and

    b. Two network devices were discovered with traffic interfaces connected outside of the ESP and management interfaces within the ESP. Because the network traffic did not pass between the traffic interfaces, which were connected to the non-ESP, and the management interfaces, which were within the ESP, URE did not consider them access points. After further examination, SERC learned that the management interfaces located within the ESP were incorrectly shown in the database as residing outside of the ESP. The described configuration was the initial system design that existed prior to the

compliance date for URE. SERC determined that URE failed to identify the network devices as access points to the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

13. URE submitted a Self-Report subsequent to identifying seven undocumented access points to an ESP. While patching some network equipment, URE discovered CCAs with a management interface outside of the ESP that should have been classified as an access point to the ESP. After further examination, SERC verified that this configuration of the management interfaces being outside of the ESP was part of the initial design. SERC determined that URE failed to designate the switches as access points to the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

14. URE submitted a Self-Report detailing two inaccurate ESP drawings found through an internal assessment of CIP-006 procedures. Door access controllers at an URE operations center were shown to reside outside the ESP when they were actually located within the ESP. SERC determined that URE failed to maintain accurate ESP drawings due to insufficient processes for the verification of Cyber Assets contained within ESPs.

15. URE self-reported an additional inaccurate ESP drawing that was found. The drawing referenced subnets that were no longer in existence. SERC determined that URE failed to maintain accurate ESP drawings due to insufficient processes for the verification of Cyber Assets contained within ESPs.

16. URE self-reported three undocumented access points to an ESP that were discovered using a new scanning method/tool. According to URE, these are legacy devices that had not been discovered in previous network scans and were in place prior to its change management process implementation. SERC determined that URE failed to identity the access points due to insufficient processes and procedures for the identification and documentation of access points to ESPs.

17. URE also self-reported two additional undocumented access points to the ESP that were discovered using the new scanning method/tool. Two servers had network connections both inside and outside of the ESP. According to URE, the access points were inadvertently created by an out-of-sequence work step. The involved personnel did not recognize that the action would create the access point. SERC determined that URE failed to designate the servers as

access points to the ESP due to insufficient processes and procedures for the identification and documentation of ESP access points.

18. URE self-reported an undocumented test network that resided within an ESP that was identified. URE's operations centers contained two racks. At the time of the incident, the servers were connected to the ESP but not being used in production. After further examination, SERC learned that the standard operating procedure (SOP) for configuring the network was based on installations prior to the CIP requirements becoming enforceable. According to URE, because the network is a private network and not externally accessible, URE did not think the devices within the network would be considered Cyber Assets. SERC determined that URE failed to update its existing SOP to include procedures for the identification of ESP Cyber Assets.

19. URE self-reported that two servers used for access control and/or monitoring of the ESPs were not afforded the protective measures specified in CIP-005 R1.5; specifically, CIP-004-1 R3 was missed. URE made the discovery while performing an internal review of its Cyber Asset inventory. According to URE, 42 users without valid PRAs had access to the servers. After further examination, SERC learned that at the time of the violation, URE's PRA process only identified users who had access to assets within an ESP. URE's PRA process failed to indentify that the individuals needed a PRA since the servers resided outside of the ESP. SERC determined that URE failed to identify the servers used to support the ESPs due to insufficient processes and procedures for the identification and documentation of such devices that reside outside of ESPs.

20. URE self-reported an undocumented Cyber Asset within an ESP that was discovered with the new scanning method/tool. According to URE, the console server was installed and was not configured correctly. After further examination, SERC learned that URE was unable to determine conclusively the history and the sequence of events regarding why the Cyber Asset was not found in previous scans. SERC determined that URE failed to designate the console server a Cyber Asset within the ESP due to insufficient processes and procedures for the identification and documentation of ESP Cyber Assets.

SERC determined that URE was in violation of CIP-005-1 R1 because it failed to ensure that all CCAs reside within an ESP and that all access points to ESPs have been identified and documented as

required.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE failed to establish the ESPs by the date it was required to be compliant with the Standard. Control center protection is paramount to the reliability of the BPS. A principal component of that protection is the establishment of ESPs. Failure to establish the ESPs on time increased the vulnerability of the control centers' CCAs. In addition, URE lacked the processes, the procedures, and the proper tools to identify and to document ESP access points, CCAs, and Cyber Assets, which greatly increased the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of numerous BPS elements.

SERC201000480 CIP-005-1 R2

CIP-005-1 R2 provides:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.1. These processes and mechanisms shall use an access control model that denies access by default, such that explicit access permissions must be specified.
> >
> > R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
> >
> > R2.3. The Responsible Entity shall maintain a procedure for securing dial-up access to the Electronic Security Perimeter(s).

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

R2.5. The required documentation shall, at least, identify and describe:

R2.5.1. The processes for access request and authorization.

R2.5.2. The authentication methods.

R2.5.3. The review process for authorization rights, in accordance with Standard CIP-004 Requirement R4.

R2.5.4. The controls used to secure dial-up accessible connections.

R2.6. Appropriate Use Banner — Where technically feasible, electronic access control devices shall display an appropriate use banner on the user screen upon all interactive access attempts. The Responsible Entity shall maintain a document identifying the content of the banner.

CIP-005-1 R2, R2.1, R2.2, R2.3 and R2.4 each have a "Medium" VRF; R2.5 and its sub-requirements and R2.6 each have a "Lower" VRF. SERC applied a "Severe" VSL.

This violation addresses multiple occurrences of CIP-005 R2. Each incident is numbered and addressed separately.

1. SERC sent URE a CIP Spot Check Notice. The SERC Spot Check Team found that URE failed to implement strong procedural/technical controls at the access points to ensure authentication of the accessing party as required by R2.4. In addition, the SERC CIP Spot Check team found that URE was unable to document that only the ports and services required for operating and monitoring Cyber Assets within the ESP had been enabled as required by R2.2.

a. According to URE, at the time of the Spot Check, it used firewall software that integrated with the EMS environment, along with the use of static IP addresses in firewall rule sets for remote user access into ESPs. Before a person could access the ESP, password authentication was required by the firewall authentication database, and the person had to use a workstation with a valid static IP address that was defined in the firewall rule set. However, after further investigation, SERC learned that the firewalls that were being used did not authenticate users at the ESP access points. SERC determined that URE did not meet the strong procedural and technical controls.

b. With regard to the second CIP Spot Check finding, SERC learned that URE's rule set on EMS firewalls allowed access into the ESP with the use of the "any port" rule, which means that all of the ports were enabled between source and destination devices, when only access to ports that are required for operating and for monitoring Cyber Assets should have been enabled. SERC determined that URE failed to enable only ports and services required for operating and for monitoring Cyber Assets within the ESP.

2. While analyzing the issues found during the CIP Spot Check, URE discovered additional firewalls that had the "any port" rule. URE submitted an addendum to its self-report. After further examination, SERC learned that URE failed to restrict access to specific ports on all of its ESP firewalls due to insufficient planning and monitoring of firewall traffic prior to the establishment of the ESPs to ensure only ports and services required for operations and for monitoring Cyber Assets within the ESPs were enabled.

3. URE self-reported that quarterly reviews of users who had access through ESP firewalls were not performed for over a year. After further examination, SERC learned that URE was not aware that it needed to perform quarterly reviews of users that have access through ESP firewalls. SERC determined that URE failed to establish and implement processes and procedures that identified what access lists needed to be reviewed on a quarterly basis.

SERC determined that URE was in violation of CIP-005 R2 because it failed to implement and document the organizational processes and technical and procedural mechanisms for control of electronic access to all electronic access points to the ESPs.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's lack of planning and processes to ensure that access points were configured per CIP Standards and access lists were reviewed, greatly increased the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900421 CIP-005-1 R3

CIP-005-1 R3 provides:

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

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

This violation addresses multiple occurrences of CIP-005 R3. Each incident is numbered and addressed separately.

URE self-reported that it had not manually reviewed the access logs of ESP access points that did not have automated invalid access attempt notification within 90 days, as required by the Standard. SERC learned that the access logs for the assets in question were within URE's substations' ESPs. The substations were part of the "Table 3" Implementation Schedule and not subject to CIP-005-1 R3 until January 1, 2010. Therefore, SERC determined that this incident was not a violation. However, before SERC was able to dismiss the violation, the following additional issues were discovered:

1. During a CIP Spot Check, the SERC Spot Check Team found that URE had failed to implement electronic or manual processes for monitoring and logging access at access points to ESPs twenty-four hours a day, seven days a week as required by the Standard. According to URE, the access points were two routers acting as firewalls. . URE explained that the two routers were not sending logs to the monitoring platform because its monitoring, logging, and alerting procedure did not contain adequate instructions on how to configure the platform to ensure that all access points have security status monitoring implemented. SERC determined that URE failed to ensure that all access points have security status monitoring implemented due to insufficient processes and procedures.
2. While analyzing the issue found during the SERC CIP Spot Check, URE identified additional ESP access points that did not have automated alerting properly configured. URE submitted addenda. According to URE, the five firewalls were sending logs to the monitoring platform but it was improperly configured and not processing the logs. SERC determined that URE failed to ensure that all access points have security status monitoring implemented due to insufficient processes and procedures.

SERC determined that URE was in violation of CIP-005 R3.2 because it failed to implement electronic or manual security monitoring processes to detect and alert for attempted or actual unauthorized access to access points.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to implement electronic or manual processes for monitoring and logging access at ESP access points could have resulted in URE not being alerted to unauthorized attempts to access ESPs. Implementing a process that alerts the appropriate personnel of attempted and/or actual unauthorized access greatly reduces the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC201000483 CIP-005-1 R4

CIP-005-1 R4 provides:

> 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:
>
> R4.1. A document identifying the vulnerability assessment process;
>
> R4.2. A review to verify that only ports and services required for operations at these access points are enabled;
>
> R4.3. The discovery of all access points to the Electronic Security Perimeter;
>
> R4.4. A review of controls for default accounts, passwords, and network management community strings; and,
>
> 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-005-1 R4 has a "Medium" VRF and a "Severe" VSL.

SERC sent URE a CIP Spot Check Notice. The CIP Spot Check team found that URE had failed to perform a CVA of the electronic access points within the ESP prior to its compliance date.

SERC learned that URE had a procedure in place that addressed the execution of a CVA as required by R4.1. According to URE, it failed to perform the CVA on the electronic access points because it thought it had a year following the compliance date to perform the CVA and still be in compliance with the Standard. SERC determined that URE in violation of CIP-005 R4 for failing to perform an annual CVA on its electronic ESP access points. URE failed to perform an annual CVA for 100% of access points to the ESP. Specifically, none of its electronic access points had been assessed.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to perform a CVA on the electronic access points to the ESPs, prior to implementation of its cybersecurity program, increased the risk of weaknesses in the security of the access points going undetected. This lack of assessment increased the risk to CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900357 CIP-006-1 R1

The purpose statement of Reliability Standard CIP-006-1 provides, in pertinent part: "Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-006-1 R1 provides:

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

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

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

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

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

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

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

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

R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

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

CIP-006-1 R1, R1.1, R1.2, R1.3, R1.4, R1.5 and R1.6 each have a "Medium" VRF; R1.7 and R1.8 each have a "Lower" VRF. SERC applied a "Severe" VSL.

This violation addresses multiple occurrences of CIP-006 R1. Each incident is numbered and discussed separately.

1. URE self-reported two incidents of escorted visitors becoming separated from their assigned URE escorts. SERC learned that URE had a procedure addressing escorted access at the time of the incidents. The first incident involved an escorted visitor at one operations center, which is a physical security perimeter (PSP). The visitor became separated from his escort after a door closed and locked behind him. The visitor did not have access to any CCA during the time of the separation, which was approximately two minutes. The second incident involved a visiting URE employee, who did not have authorized unescorted access to a PSP in an operations center. The designated escort allowed the visiting URE employee to borrow his physical access card in order to use the restroom, which was outside of the PSP. The visiting URE employee was unescorted in the PSP for approximately one minute. SERC determined that URE failed to maintain a physical security plan.
2. URE self-reported that it did not have PSP drawings in place before the enforceable date for URE. After reviewing URE's procedure, SERC learned that PSP drawings are a part of its physical security plan. SERC determined that URE failed to create a complete physical security plan addressing all Cyber Assets within an ESP and the identification of all physical access points through each PSP by its compliance date.
3. URE self-reported that a PSP drawing was not updated within 30 calendar days of the completion of a physical security system redesign or reconfiguration, as required by the Standard. After further examination, SERC learned that URE redefined the PSPs at an operation center due to the mitigation of a technical feasibility exception (TFE). The server room was removed as a PSP because it did not contain any CCAs. URE did not update the PSP drawing until a month later. SERC determined that URE failed to maintain a physical security plan

because it did not update the physical security plan within thirty calendar days of the completion of any physical security system redesign.

4. URE self-reported an inaccurate PSP drawing. After further examination, SERC learned that the PSP border and a door at an operations center had been incorrectly depicted since the mandatory and enforceable date. SERC determined that URE failed to create a complete physical security plan addressing all Cyber Assets within an ESP and the identification of all physical access points through each PSP by its compliance date.

5. During the CIP Spot Check, the SERC CIP Spot Check team found two instances where a PSP did not have the required enclosed six-wall border or alternative measures where a complete enclosure was not physically possible. After further examination, SERC learned that the first instance involved an operations center. One of the operation center's walls did not extend to the building roof; thus, an enclosed six-wall border was not established. The second instance involved an operation center, which had ESP wiring above the suspended ceiling in the foyer area, which was not inside any of the operation center's defined PSPs. While URE had alternative measures in place to control physical access to the Cyber Assets, it had failed to document them. SERC determined that URE failed to maintain a physical security plan to ensure that all Cyber Assets within an ESP reside within an identified PSP.

6. While analyzing the incident identified in the CIP Spot Check, URE discovered additional PSPs that did not have the required enclosed six-wall border or alternative measures where a complete enclosure was not physically possible. URE submitted addendums to the Spot Check. After further examination, SERC learned that larger gaps were identified at three operation centers. Smaller gaps were located at multiple operation centers. SERC determined that URE failed to maintain a physical security plan to ensure that all Cyber Assets within an ESP reside within an identified PSP.

7. URE self-reported two incidents of escorted visitors becoming separated from their assigned URE escorts. After further examination, SERC learned that the first incident involved two contractors at a backup control center. One contractor had authorized unescorted access, the second did not. The escorted contractor, who was conducting routine maintenance activities, used the authorized contractor's physical access card to gain entry to the PSP. While in the PSP, his activity was monitored via two cameras. According to URE, no malicious activity occurred. The second incident involved a contracted security officer, who did not have authorized

unescorted access right. While in the PSP, his activity was monitored and logged via a camera. SERC determined that URE failed to maintain a physical security plan.

8. URE self-reported an incident of an escorted visitor becoming separated from his assigned URE escort when the escort left the visitor in the break room while the URE escort went to use the restroom. After further examination, SERC learned that the incident occurred at an operations center, which is a PSP. The visitor did not have access to any CCAs during the time of the separation, which was approximately two minutes. SERC determined that URE failed to maintain a physical security plan.
9. URE self-reported an incident of an escorted visitor becoming separated from his assigned URE escort when the visitor left the escort and went unaccompanied to the bathroom. After further examination, SERC learned that the incident occurred at an operations center, which is a PSP. The visitor did not have access to any CCAs during the time of the separation, which was approximately five minutes. SERC determined that URE failed to maintain a physical security plan.
10. URE self-reported that Cyber Assets used in access control and monitoring of PSPs had not been afforded all the protective measures specified in CIP-007 and CIP-009. After further examination, SERC learned that the security access controller system had not been classified as part of URE's physical access control system. Because of this, they had not been afforded the protections of CIP-007 and CIP-009. SERC determined that URE failed to maintain a physical security plan to ensure that Cyber Assets used in the access control and monitoring of the PSPs shall be afforded the protective measures specified in CIP-003 through CIP-009.

SERC determined that URE was in violation of CIP-006 R1 because it failed to maintain a physical security plan.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because the number of instances of incomplete six-wall borders in conjunction with the untimely and incorrect PSP drawings hindered URE's ability to protect its CCAs. An incomplete physical security plan

coupled with non-continuous escorted access increased the risk of the CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900393 CIP-006-1 R3

CIP-006-1 R3 provides:

> R3. Monitoring Physical Access — The Responsible Entity shall document and implement the technical and procedural controls for monitoring physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. Unauthorized access attempts shall be reviewed immediately and handled in accordance with the procedures specified in Requirement CIP-008. One or more of the following monitoring methods shall be used:
>
> > R3.1. Alarm Systems: Systems that alarm to indicate a door, gate or window has been opened without authorization. These alarms must provide for immediate notification to personnel responsible for response.
> >
> > R3.2. Human Observation of Access Points: Monitoring of physical access points by authorized personnel as specified in Requirement R2.3.

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

This violation addresses multiple occurrences of CIP-006 R3. Each incident is numbered and discussed separately.

1. URE self-reported a violation of CIP-006 R3. According to URE, its door controller security system ceased functioning. This system controls and monitors physical access to PSPs. SERC learned that URE's door controller security system was not issuing alerts; therefore, URE personnel would not have been notified regarding unauthorized physical access attempts. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

2. URE submitted an addendum to the Self-Report regarding the discovery of 11 exterior windows in a PSP that were not monitored for physical access attempts. After further examination, SERC learned that the PSP was surrounded by a fence with a key pad access motor-operated gate. While there were no cameras monitoring the exterior windows, the PSP is located in a facility that is manned twenty-four hours a day, seven days a week. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

3. While preparing for its CIP Spot Check, URE discovered that it did not have evidence to verify that immediate reviews of unauthorized physical access attempts were being performed. The same day as the discovery, URE submitted an addendum to the Self-Report. After further examination, SERC learned that four out of 13 PSPs were involved. No CIP-008 cyber security incidents had been reported. SERC determined that URE failed to immediately review unauthorized access attempts.

4. URE discovered a malfunctioning PSP door at an operation center. URE submitted an addendum to its self-report. After further examination, SERC learned that this was an internal door off a second floor non-PSP foyer located in a building that is surrounded by a fence and a card access motor-operated gate. The malfunctioning door was reported at 7 a.m. At 11:30 a.m. the malfunctioning door allowed a delivery person, who had been granted access to the non-PSP foyer, to pull the malfunctioning door open and enter the PSP without escorted access. The malfunctioning door was fixed before the close of business that day. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

5. URE discovered that four PSP doors were not being monitored for physical access attempts. URE submitted an addendum to its self-report. After further examination, SERC learned that the four doors were not generating alarms because they had not been configured to allow an alarm to be generated if unauthorized physical access was attempted. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

6. URE discovered an exterior PSP window that was not being monitored for physical access attempts. URE submitted an addendum to its self-report. After further examination, SERC learned that this was an interior window located on the second floor at the PSP, which is

monitored twenty-four hours a day, seven days a week. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

7. URE self-reported that it did not have evidence to verify that all unauthorized physical access alerts were being immediately reviewed. After further examination, SERC learned that URE could not verify that f1.1% of alarms were responded to immediately. The incidents involved 17.6% of URE PSPs. According to URE, there was no unauthorized physical entry and no CIP-008 cyber security incidents. SERC determined that URE failed to immediately review unauthorized physical access alerts.

8. URE self-reported two instances of its PSP access control system failing to provide automated alerting of potential unauthorized access attempts. According to URE, the instances were found while performing internal reviews of the access control system. After further examination, SERC learned that both instances involved the master access control server. In the first instance, the master access control server lost connectivity to a local door access controller for thirty-six hours. In the second instance, the master access control server lost connectivity to a local door access controller for seventy-two hours. URE was unable to conclusively determine the reason for the master access control's failure. SERC determined that URE failed to monitor physical access at all access points to its PSPs twenty-four hours a day, seven days a week.

9. URE self-reported that it failed to immediately review an unauthorized physical access alert. After further examination, SERC learned that the alert was a false alarm that occurred as a result of a known problem. The proximity of the operation center's glass door to the switch room door causes the sensor to continually register false alarms. According to URE, there was no unauthorized physical entry and no CIP-008 cyber security incidents. SERC determined that URE failed to immediately review unauthorized physical access alerts.

10. URE self-reported that it did not have evidence to verify that all unauthorized physical access attempt alarms were reviewed immediately. A periodic review of physical security event logs found 11 instances where an unauthorized physical access alert was not immediately reviewed. After further examination, SERC learned that one PSP was involved. According to URE, there were no CIP-008 cyber security incidents. SERC determined that URE failed to immediately review unauthorized physical access alerts.

SERC determined that URE was in violation of CIP-006-1 R3 for failing to monitor physical access at all access points to the PSP twenty-four hours a day, seven days a week and to immediately review unauthorized physical access alerts.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. The lack of monitoring physical access at all access points to the PSPs twenty-four hours a day, seven days a week, the numerous failures to generate unauthorized access alerts, and the number of instances of unauthorized physical access alerts that were not immediately reviewed significantly jeopardized the CCAs residing within the subject PSPs. Failure to monitor the PSPs and/or immediately respond to alerts could have allowed unauthorized persons to access CCAs, which greatly increased the risk of the CCAs being compromised and/or rendered inoperable.

SERC201000627 CIP-006-1 R4

CIP-006-1 R4 provides:

> R4. Logging Physical Access — Logging shall record sufficient information to uniquely identify individuals and the time of access twenty-four hours a day, seven days a week. The Responsible Entity shall implement and document the technical and procedural mechanisms for logging physical entry at all access points to the Physical Security Perimeter(s) using one or more of the following logging methods or their equivalent:
>
> > R4.1. Computerized Logging: Electronic logs produced by the Responsible Entity's selected access control and monitoring method.
> >
> > R4.2. Video Recording: Electronic capture of video images of sufficient quality to determine identity.

R4.3. Manual Logging: A log book or sign-in sheet, or other record of physical access maintained by security or other personnel authorized to control and monitor physical access as specified in Requirement R2.3.

CIP-006-1 R4 has a "Medium" VRF and a "Lower" VSL.

This violation addresses multiple occurrences of CIP-006 R4. Each incident is discussed separately.

1. URE self-reported a violation of CIP-006 R4 due to unescorted access being granted to a PSP without logging the access. According to URE, the issue was discovered, when the PSP site access administrator performed an internal audit of the site visitor logs. One of the PSP sites, an operations center, did not log all of the entries to the PSP made by two janitors, who are contract employees. SERC verified that the janitors did not sign the log for four months, when the janitors began signing the visitor log. The janitors' official duties were trash collection every evening and vacuuming once per week. The janitors had not been assigned cleaning duties in areas where CCAs were not manned by URE employees twenty-four hours a day, seven days a week. Trash collection and other cleaning activities where CCAs are not manned twenty-four hours a day, seven days a week, are handled by URE employees at the operations center. SERC determined that URE failed to log sufficient information to uniquely identify two individuals and the times of access at one PSP location.
2. URE self-reported that it was unable to uniquely identify an individual's physical access because the individual borrowed another employee's keycard to obtain re-entry into the PSP. After further examination, SERC learned that the two URE employees work inside the same PSP. The first employee's keycard had been left at home. Instead of following URE's manual sign-in process, the first employee borrowed the second employee's physical access keycard to gain access to the PSP. SERC determined that URE failed to uniquely identify an individual and the time of access week at one PSP.

SERC determined that URE was in violation of CIP-006-1 R4 because it failed to uniquely identify three individuals and the time of access twenty-four hours a day, seven days a week.

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

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. For the first occurrence, there were no CCAs in the areas in which the two janitors worked and the site was manned twenty-four hours a day, seven days a week. For the second occurrence, the employees who shared the access card were both authorized to have PSP access and had valid PRAs and cyber security training.

SERC201000486 CIP-006-1 R5

CIP-006-1 R5 provides: "Access Log Retention — The responsible entity shall retain physical 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."

CIP-006-1 R5 has a "Lower" VRF and a "Moderate" VSL.

URE self-reported that it did not have electronic PSP access logs for approximately one month for an operations center.

URE discovered the issue while preparing for the CIP Spot Check. According to URE, the operations center's logging server had stopped logging physical access for approximately one month. SERC learned that URE's procedures did not include archiving the logs, which is why URE had no indication the logs were missing. While URE was unable to conclusively determine what caused the server to stop logging, no CIP-008 cyber security incidents had been reported during the applicable time period.

SERC learned that the PSP has four cameras. The cameras are visible to control room personnel but do not record activity. The control room is manned twenty-four hours a day, seven days a week. The PSP has no guards. Manual visitor logs were maintained and retained for the specified time period. In addition, the PSP card reader access system functioned properly during the timeframe of the missing logs.

SERC determined that URE was in violation of CIP-006 R5 because it failed to retain physical access logs for at least ninety calendar days at one location.

SERC determined the duration of the violation to be from when the logging server stopped logging, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. URE had four cameras that were visible to control room personnel and manual copies of visitor logs that would assist with the possible detection and investigation of security incidents. In addition, the primary purpose of the missing electronic PSP logs is for documentation in the case of a security event per CIP-008. URE had no CIP-008 security events during the timeframe of this violation.

SERC201000484 CIP-006-1 R6

CIP-006-1 R6 provides:

> R6. Maintenance and Testing — The Responsible Entity shall implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly. The program must include, at a minimum, the following:
>
> > R6.1. Testing and maintenance of all physical security mechanisms on a cycle no longer than three years.
> >
> > R6.2. Retention of testing and maintenance records for the cycle determined by the Responsible Entity in Requirement R6.1.
> >
> > R6.3. Retention of outage records regarding access controls, logging, and monitoring for a minimum of one calendar year.

CIP-006-1 R6 has a “Medium” VRF and a “Severe” VSL.

SERC sent URE a CIP Spot Check Notice. The SERC CIP Spot Check team identified a violation of CIP-006-1 R6 for failing to implement a maintenance and testing program to ensure that all physical security systems under Requirements R2, R3, and R4 function properly.

SERC learned that URE had a documented maintenance and testing program by the enforceable date for URE, but had failed to complete the initial maintenance and testing of its physical security systems prior to the enforceable date.

SERC determined that URE was in violation of CIP-006-1 R6 for failing to implement a maintenance and testing program to ensure that all physical security systems defined under CIP-006-1 R2, R3, and R4 function properly.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE's failure to test its physical security systems to ensure they functioned properly before its compliance date greatly increased the risk of unidentified problems going undetected. Undetected problems with the physical security systems increased the risk of CCAs being compromised and possibly rendered inoperable, which could have resulted in a loss of monitoring and/or control of the BPS. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900310 CIP-007-1 R1

The purpose statement of Reliability Standard CIP-007-1 provides in pertinent part: "Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-007-1 R1 provides:

> R1. Test Procedures — The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> > R1.1. 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-007-1 R1 and R1.1 each have a "Medium" VRF; R1.2 and R1.3 each have a "Lower" VRF. SERC applied a "Severe" VSL.

This violation addresses multiple occurrences of CIP-007 R1. Each incident is numbered and discussed separately.

1. URE self-reported that the cyber security test procedure did not meet the requirements of CIP-007 R1. While URE had a test procedure in place, SERC learned that it did not cover all of the Cyber Assets within ESPs. SERC determined that URE failed to establish test procedures for all Cyber Assets within ESPs.
2. During the CIP Spot Check, the SERC CIP Spot Check team found that URE's test procedure did not cover testing for Cyber Assets not monitored by its change monitoring tool. After further examination, SERC confirmed the CIP Spot check team's finding and learned that 16 device

types did not have testing procedures. SERC determined that URE failed to establish test procedures for all Cyber Assets within ESPs.

SERC determined that URE was in violation of CIP-007 R1 because it failed to establish test procedures for all Cyber Assets within ESPs.

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

SERC determined that this violation posed a moderate risk and did not pose a serious or substantial risk to the reliability of the BPS. URE's failure to establish test procedures for all Cyber Assets within ESPs could have adversely affected existing cyber security controls, resulting in CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS. The violation did not pose a serious or substantial risk to the reliability of the BPS because some of the Cyber Assets within the ESP were subject to the test procedures used by the software.

SERC200900312 CIP-007-1 R2

CIP-007-1 R2 provides:

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

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

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

This violation addresses multiple occurrences of CIP-007 R2. Each incident is numbered and discussed separately.

1. URE self-reported the discovery of 82 Cyber Assets included within an ESP that had not been evaluated to ensure that only those ports and services necessary for normal or emergency operations had been enabled. SERC learned that URE's database inventory list was incomplete. The database is used to document all critical and non-critical Cyber Assets and access points to the ESPs. This omission meant that the ports and services on these Cyber Assets were not assessed in accordance with the Standard. SERC determined that URE failed to establish a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.
2. During the CIP Spot Check, the SERC CIP Spot Check Team found that URE failed to establish and document a process to ensure that only ports and services required for normal and emergency operations were enabled. Specifically, a port that had security vulnerabilities was found to be opened. While URE had a procedure in place, SERC learned that it did not contain sufficient language regarding how URE would establish which ports and services needed to be enabled for normal and emergency operations. SERC determined that URE failed to ensure that only those ports and services that are required for normal and emergency operations are enabled.
3. URE self-reported Cyber Assets that were discovered as a result of URE's CVA. After further examination, SERC learned that these Cyber Assets were not a part of the database. As a result, the ports and services were not assessed in accordance with the Standard. SERC determined that URE failed to establish a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.
4. URE self-reported the discovery of additional Cyber Assets that did not have ports and services evaluated. The discovery was made while performing the mitigation activities for the original violation. After further examination, SERC learned that these Cyber Assets were not a part of

the database. As a result, the ports and services were not assessed in accordance with the Standard. SERC determined that URE failed to establish a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.

5. URE self-reported the discovery of a port that was enabled but not necessary for normal and emergency operations. After further examination, SERC learned that an attempt to uninstall an antivirus program seven years prior was unsuccessful and a remnant was left. The antivirus program service started and enabled a port. SERC determined that URE failed to establish a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.

SERC determined that URE was in violation of CIP-007 R2 because it failed to establish a process to ensure that only those ports and services that are required for normal and emergency operations are enabled.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. The unassessed ports and services left Cyber Assets and CCAs within the ESPs open to security vulnerabilities. This could have resulted in CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900313 CIP-007-1 R3

CIP-007-1 R3 provides:

> R3. Security Patch Management — The Responsible Entity, either separately or as a component of the documented configuration management process specified in CIP-003 Requirement R6, shall establish and document a security patch management program for tracking, evaluating, testing, and installing applicable cyber security software patches for all Cyber Assets within the Electronic Security Perimeter(s).

R3.1. The Responsible Entity shall document the assessment of security patches and security upgrades for applicability within thirty calendar days of availability of the patches or upgrades.

R3.2. The Responsible Entity shall document the implementation of security patches. In any case where the patch is not installed, the Responsible Entity shall document compensating measure(s) applied to mitigate risk exposure or an acceptance of risk.

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

This violation addresses multiple occurrences of CIP-007 R3. Each incident is numbered and discussed separately.

1. URE self-reported that documentation confirming the required evaluations of security patches within 30 days of their release was not available. While URE had a patch management program in place, SERC learned that it lacked specific instructions for performing and documenting security patch evaluations. According to URE, 254 security patches had not been reviewed within 30 days after their release. SERC determined that URE failed to establish and implement a security patch management program for tracking, evaluating, and installing applicable cyber security software patches for all Cyber Assets within the ESP.
2. URE submitted an addendum to its self-report after discovering that three security patches had not been evaluated within the required 30 days after their release. After further examination, SERC learned that the security patches were missed because URE's database inventory list was incomplete. URE's database is used to document all critical and non-critical Cyber Assets and access points to the ESPs. Because the database inventory list was incomplete, the security patches for these Cyber Assets were not assessed in accordance with the Standard. SERC determined that URE failed to establish and implement a security patch management program for all Cyber Assets within the ESPs.
3. URE self-reported that an upgrade to the server that downloads security patches identified 21 additional security patches that had not been evaluated within the required 30 days after their release. After further examination, SERC learned that the patching server update identified a

previously unknown database error. When corrected, the server downloaded the 21 patches that had not been evaluated. While URE had a security patch management procedure, it did not address maintaining the patching server or instructions for verifying that the patches had been downloaded and were ready to review. SERC determined that URE failed to establish and implement a security patch management program for all Cyber Assets within the ESPs.

4. URE self-reported that two security patches had not been evaluated within the required 30 days after their release. After further examination, SERC learned that these two devices were not included in URE's database. Therefore, they did not have security patches evaluated in accordance with the Standard. SERC determined that URE failed to establish and implement a security patch management program for all Cyber Assets within the ESPs.

5. URE's Self-Report contained two separate incidents of security patches that were available but had not been reviewed within the required 30 days. After further examination, SERC learned that the first incident was discovered while URE was reviewing security patch upgrades. An application had three security patches available, but they had not been evaluated. The discovery of the second incident was made while performing the mitigation activities for the previous Self-Reports. After further examination, SERC learned that one security patch had not been evaluated. The patches for both incidents were missed because URE's database inventory list was incomplete. Because of this, the security patches for these Cyber Assets were not evaluated in accordance with the Standard. SERC determined that URE failed to establish and implement a security patch management program for all Cyber Assets within the ESPs.

6. URE self-reported that it had not evaluated security patches for Cyber Assets within the required 30 days of their release. After further examination, SERC learned that a firmware upgrade was available but had not been assessed because the Cyber Assets were originally part of a staging network that was later connected to an ESP. URE's patching program failed to provide adequate guidance in these types of situations. SERC determined that URE failed to establish and implement a security patch management program for all Cyber Assets within the ESPs.

SERC determined that URE was in violation of CIP-007 R3 because it failed to establish a security patch management program for tracking, evaluation, testing, and installing applicable cyber security software patches for all Cyber Assets within the ESPs.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to establish a patch management program for all Cyber Assets within ESPs left the Cyber Assets susceptible to security vulnerabilities. This could have resulted in CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC201000688 CIP-007-1 R4

CIP-007-1 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 or an acceptance of risk.
> >
> > 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-007-1 R4 has a "Medium" VRF and a "High" VSL.

This violation addresses multiple occurrences of CIP-007 R4. Each incident is numbered and discussed separately.

1. URE self-reported a violation of CIP-007-1 R4.2 due to two servers not having updated antivirus signatures. According to URE, the problem was discovered while using an assessment tool to troubleshoot issues related to CIP-007 R1. SERC reviewed URE's documented process and learned that the virus scanner on the first server had failed; therefore, the server's antivirus signatures were not being updated. Because attempts to restart the server's virus scanner failed, URE reviewed the error logs, which revealed that the antivirus software needed to be reinstalled. According to the error logs, the antivirus services had stopped on the server. The second server was running an outdated version of antivirus software and was, therefore, not receiving updated antivirus signatures since the date of compliance. The second server was not being used in production but had not yet been decommissioned. URE was unable to determine why the server was not included in its tool which is used to determine the servers that need an updated version of the antivirus software. Because of this, the server was missed. In addition, URE found no other antivirus issues on other CIP governed servers. SERC determined that URE failed to use malware and antivirus protection tools.

2. URE self-reported that 82 Cyber Assets within its ESP did not have malware protection installed. After further examination, SERC learned that Cyber Assets were missing from URE's database. URE's database is used to document all critical and non-critical Cyber Assets and access points to the ESP pursuant to CIP-005-1 R1.6. Because URE failed to have a complete and accurate list of Cyber Assets located within ESPs, it was impossible for URE to ensure that all Cyber Assets had malware and antivirus prevention tools installed. SERC determined that URE failed to use malware and antivirus protection tools.

3. URE self-reported that ten Cyber Assets within its ESP did not have malware protection installed. After further examination, SERC learned that the additional Cyber Assets were not in the database. Because URE failed to have a complete and accurate list of Cyber Assets within ESPs, it was impossible for URE to ensure that all Cyber Assets had malware and antivirus prevention tools installed or a TFE filed. SERC determined that URE failed to use malware and antivirus protection tools.

4. While developing TFE re-submittals, URE self-reported the discovery of 55 devices that could not support the installation of malware protection. After further examination, SERC learned that URE's TFE process did not identify all devices requiring a TFE. Because of this, URE was unable to ascertain the total population of devices that needed a TFE due to the devices'

> inability to support the installation of malware and antivirus prevention tools. SERC determined that URE failed to file a TFE on the inability to install malware and antivirus protection tools on the identified devices.

SERC determined that URE was in violation of CIP-007 R4 for failing to use antivirus and malware prevention tools, or compensating measures implemented on at least 10% but less than 15% or more Cyber Assets within the ESP. 14.5% of the Cyber Assets did not use antivirus and malware prevention tools, nor had compensating measures implemented.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to use or update antivirus and malware prevention tools could have exposed CCAs to viruses and malware. Viruses and malware could have rendered the CCAs compromised and/or inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900315 CIP-007-1 R5

CIP-007-1 R5 provides:

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

R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.

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

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

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

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

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

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

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

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

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

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

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

This violation addresses multiple occurrences of CIP-007 R5. Each incident is numbered and discussed separately.

1. URE self-reported that some Cyber Assets within ESPs did not have passwords with parameters as required by R5.3.2. After further examination, SERC learned that URE's database, which is used to document all critical and non-critical Cyber Assets and access points to URE's ESPs that have been identified, was incomplete and did not contain the complete list of CCAs. Without the proper identification of critical and non-critical Cyber Assets as required by CIP-002-1 R3 and CIP-005-1 R.1.4, URE failed to have a complete and accurate list of Cyber Assets within ESPs. Therefore, it was impossible for URE to ensure that all Cyber Assets within its ESPs had the password parameters.
2. URE submitted an addendum to its self-report after discovering administrator, shared, and other generic accounts that had not been managed as required in CIP-007-1 R5.2 and did not have enhanced passwords as required by CIP-007-1 R5.3. While URE had a policy in place, it did not address the requirements of CIP-007-1 R5.2 and R5.3. SERC determined that URE failed to establish, implement and document account management controls.
3. URE self-reported that an audit trail did not exist for two shared accounts that were part of URE's Physical Access control system, as required by CIP-006-1 R1.8. Specifically, CIP-007-1 R5.2.3 was missed. The incident was discovered while URE was preparing for its CIP Spot

Check. According to URE, the two shared accounts were associated with a card access system and a surveillance camera management system. After further examination, SERC learned that these assets cannot support the automatic logging of account use. While URE had a policy for managing the use of the shared accounts, it did not address manual logging. SERC determined that URE failed to maintain an audit trail for the two shared accounts due to insufficient processes and procedures for account management.

4. URE submitted an addendum to its self-report after it discovered that a group password for EMS consoles had been distributed to personnel who had CIP Training and valid PRAs, but did not have a need to know the password. After further examination, SERC learned the group password was stored in a password database that houses other passwords. While the individuals had a need to know the other passwords, they were not on a need-to-know basis for the EMS console group password. SERC determined that URE failed to comply with the need-to-know concept.
5. URE self-reported a possible violation as a result of URE's CVA. The Cyber Assets were physically but not logically connected with an ESP. Because these devices were not identified as Cyber Assets within the applicable ESP, they did not have enhanced passwords.
6. URE self-reported two incidents regarding the lack of enhanced passwords. The first incident involved a password associated with a generic ID. This incident was discovered when URE was troubleshooting an issue with the configuration management application. SERC learned that the password did not employ the use of special characters. The second incident was discovered while investigating information for a TFE filing. An administrative password that was in use did not meet the enhanced password requirement. SERC determined that URE failed to implement enhanced passwords.

SERC determined that URE was in violation of CIP-007 R5 because it failed to establish, implement and document account management controls.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE's failure to implement procedures to minimize and to manage the scope and use of shared accounts and failure to implement enhanced passwords on all Cyber Assets within ESPs greatly increased the risk to CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS. In addition, this violation lasted for about one and a half years and involved multiple incidents, numerous CCAs and shared accounts.

SERC200900314 CIP-007-1 R6

CIP-007-1 R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.
> >
> > R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008.
> >
> > R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

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

This violation addresses multiple occurrences of CIP-007 R6. Each incident is numbered and discussed separately.

1. URE self-reported Cyber Assets located within an ESP that had not been included in its security status monitoring process. SERC learned that URE's database, which is used to document all critical and non-critical Cyber Assets and access points to the ESPs, was built from importing and consolidating information from many different spreadsheets and sources. According to URE, the database inventory list was incomplete when the security monitoring asset list was originally created, which led to the omission of the Cyber Assets from URE's security monitoring asset list. SERC determined that URE failed to include the Cyber Assets in its security monitoring process due to insufficient processes and procedures for the identification and documentation of Cyber Assets.
2. During the CIP Spot Check, URE could not produce CIP-007 R6 logs for all Cyber Assets within URE's ESP. The SERC CIP Spot Check team discovered several systems that were not sending logs to URE's monitoring tool, which is used to monitor system events related to cyber security. URE explained that the systems at issue were not sending logs to the tool because its monitoring, logging, and alerting procedure did not contain adequate instructions on how to configure the tool to ensure that all Cyber Assets within URE's ESPs have security status monitoring implemented. SERC determined that URE failed to ensure that all Cyber Assets within URE's ESPs have security status monitoring implemented due to insufficient processes and procedures.
3. While analyzing the incident identified in the CIP Spot check, URE discovered Cyber Assets that were being monitored by another of URE's tools neither had alerts configured nor logs being manually reviewed. URE submitted an addendum to its self-report. The Cyber Assets were server and switchers. According to URE, its monitoring, logging, and alerting procedure lacked instructions to ensure that all newly added Cyber Assets had the appropriate security status monitoring implemented. SERC determined that URE failed to include the Cyber Assets in its

security monitoring process due to insufficient processes and procedures for the identification and documentation of Cyber Assets.

4. While analyzing the incident from the addendum, URE discovered additional Cyber Assets that did not have automated alerting for cyber security events enabled. URE self-reported this incident. According to URE, the Cyber Assets were missed because its monitoring, logging, and alerting procedure lacked instructions to ensure that all newly added Cyber Assets had the appropriate security status monitoring implemented.

5. URE self-reported nine undocumented Cyber Assets that were discovered as a result of its CVA. Because the Cyber Assets had not been identified and documented as part of the ESP, they had not been monitored for system events related to cyber security.

6. URE self-reported nine communication processors that could not log security events. The communication processors were found while investigating mitigating actions associated with URE's CIP-007 R6 TFE filing. URE's original TFE filing failed to include these devices.

7. During preparations for an ESP reconfiguration at one of URE's control centers, three operator consoles were identified that did not have automated alerting for cyber security events enabled. URE self-reported the discovery on the same day. After further examination, SERC learned that URE had gathered data i in order to respond to an audit Request for Information (RFI) regarding the implementation of the CIP Requirements. At that time, the data indicated that the operator consoles were being monitored. However, the tracking spreadsheet did not have the operator consoles listed. URE was unable to determine conclusively the cause of the disparity between the two sets of data. SERC determined that URE failed to include the Cyber Assets in its security monitoring process due to insufficient processes and procedures for the identification and documentation of Cyber Assets.

8. URE self-reported an additional 73 Cyber Assets that did not have security status monitoring. After further examination, the Cyber Assets were discovered while URE was reconciling data in the database with the monitoring tool. SERC determined that URE failed to ensure that all of the Cyber Assets within URE's ESPs had security status monitoring implemented due to insufficient processes and procedures.

9. URE self-reported 37 devices that cannot support the installation of security status monitoring tools as required by CIP-007 R6. The devices were found while investigating mitigating actions

associated with URE's CIP-005 R2 TFE filing. URE's original TFE filing failed to include these Cyber Assets.

10. URE self-reported two incidents regarding Cyber Assets that were not uploading security logs to the monitoring tool's server. The first incident involved a switch. The second incident involved four servers. The Cyber Assets were discovered during the TFE review with the SERC CIP Audit staff. After further investigation, SERC learned the switch had stopped logging information to the monitoring tool's server due to a firmware upgrade. With regard to the second incident, the four servers did not transfer security logs to the monitoring tool's server and therefore, alerting did not take place. It should be noted that the security logs were retained on the servers. According to URE, the security logs were not being sent because a password change prevented the servers and the monitoring tool's server from communicating. After further examination, SERC learned that the alert for "No logs within a specified timeframe" had been disabled by URE because the lack of events for Cyber Assets was generating a significant number of false positives, inundating technical support personnel. SERC determined that URE failed to ensure that all Cyber Assets within its ESPs, as technically feasible, had processes and procedures to monitor system events that are related to cyber security.

11. URE self-reported that its monitoring tool ceased functioning. The monitoring tool was rebooted and returned to normal operation three days later. During the time of the malfunction, all logging and alerting of supported device types would not have been captured unless the devices were capable of storing their logs locally. After further examination, SERC learned that the event parser tool had been disabled. The event parser is responsible for the disposition of the events captured by the monitoring tool, which would temporarily store, analyze, and process alerts for each event. Because the parser tool was disabled, the monitoring tool was capturing events from systems that report to it, storing them in the temporary folder, but not processing them. The lack of processing caused the file system to become full and to stop working. SERC determined that URE failed to ensure that all Cyber Assets within the ESPs, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

SERC determined that URE was in violation of CIP-007 R6 because it failed to ensure that all Cyber Assets within the ESPs, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS. URE's failure to monitor system events that are related to cyber security for its Cyber Assets within the ESPs could have resulted in a security breach going undetected. An undetected security breach may have rendered CCAs inoperable, resulting in the loss of monitoring and control of the BPS. In addition, URE's failure to log system events related to security events could have impaired its ability to conduct an incident response. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC201000577 CIP-007-2a R6

CIP-007-2a R6 provides:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> > R6.1. The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for monitoring for security events on all Cyber Assets within the Electronic Security Perimeter.
> >
> > R6.2. The security monitoring controls shall issue automated or manual alerts for detected Cyber Security Incidents.

R6.3. The Responsible Entity shall maintain logs of system events related to cyber security, where technically feasible, to support incident response as required in Standard CIP-008-2.

R6.4. The Responsible Entity shall retain all logs specified in Requirement R6 for ninety calendar days.

R6.5. The Responsible Entity shall review logs of system events related to cyber security and maintain records documenting review of logs.

CIP-0072-2a R6 has a "Lower" VRF and a "Severe" VSL.

This violation addresses multiple occurrences of CIP-007 R6. Each incident is numbered and discussed separately.

1. URE self-reported the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. SERC learned that three outages occurred on a server that is used to monitor and log system events related to cyber security from Cyber Assets located within ESPs. These outages were caused by the server rebooting after the installation of cyber security patches as required by CIP-007 R3. The outages occurred two separate dates and ranged from two to ten minutes each. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.
2. URE self-reported the potential loss of monitoring and logging of system events for Cyber Assets located within an ESP. SERC learned that three outages occurred on a server that is used to monitor and log system events related to cyber security from Cyber Assets located within ESPs. These outages took place when URE personnel were attempting to install antivirus software as required by CIP-007 R4. The outages were approximately 30 minutes each. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.
3. URE submitted an addendum to its self-report addressing the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. SERC learned that three outages

occurred on a server that is used to monitor and log system events related to cyber security from Cyber Assets located in ESPs. These outages occurred on three separate days. The first outage occurred when a firewall rule change prevented the logging server from being able to communicate to Cyber Assets located in other ESPs. The outage lasted approximately 15 minutes. The second outage was caused by the logging server rebooting after emergency maintenance. The outage lasted approximately three minutes. The third outage was caused by the server rebooting after the installation of cyber security patches as required by CIP-007 R3. The outage lasted approximately four minutes. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.

4. URE submitted an addendum to its self-report addressing the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. SERC learned that the outage was caused by the logging server rebooting after the installation of a patch. The outage lasted approximately eight minutes. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.

5. URE submitted an addendum to its self-report addressing the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. The outage occurred when a patch was installed on the logging server and the installation required a reboot. The outage lasted approximately three minutes. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.

6. URE submitted an addendum to its self-report addressing the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. SERC learned that the outage was caused by the logging server rebooting after the installation of a patch. The outage lasted approximately nine minutes. URE did not detect any cyber security events during the outages. SERC determined that URE failed to monitor system events that are related to cyber security for the aforementioned incidents.

7. URE submitted an addendum to its self-report addressing the potential loss of monitoring and logging of system events for Cyber Assets located within ESPs. SERC learned that the two outages occurred when maintenance was performed on a data center firewall that prevented

the logging server from being able to communicate to Cyber Assets located in other ESPs. The outages lasted 17 minutes and 25 minutes, respectively. URE did not detect any cyber security events during the outages. SERC determined that URE to monitor system events that are related to cyber security for the aforementioned incidents.

SERC determined that URE was in violation of CIP-007 R6 for failing to monitor system events that are related to cyber security for the aforementioned incidents.

SERC determined the duration of the violation to be from the date of the first outage through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS. While URE had implemented monitoring and logging of security events on all Cyber Assets within the ESP, its failure to continuously monitor system events that are related to cyber security for its Cyber Assets within the ESPs could have resulted in a security breach going undetected. An undetected security breach may have rendered CCAs inoperable, resulting in the loss of monitoring and control of the BPS. In addition, URE's failure to log system events related to security events could have impaired its ability to conduct an incident response.

SERC201000485 CIP-007-1 R7

CIP-007-1 R7 provides in pertinent part: "R7. Disposal or Redeployment — The Responsible Entity shall establish formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the Electronic Security Perimeter(s) as identified and documented in Standard CIP-005."

CIP-007-1 R7 has a "Lower" VRF and a "Moderate" VSL.

SERC sent URE a CIP Spot Check Notice. The CIP Spot Check team found that URE's disposal and redeployment procedure did not contain an acceptable data cleansing method for the redeployment of Cyber Assets in order to prevent unauthorized retrieval of sensitive cyber security or reliability data.

While reviewing the applicable procedure, SERC observed that URE incorrectly stated that a reformat of disks was an acceptable data cleansing method for the disposal and the redeployment of Cyber Assets, instead of an industry accepted practice like a factory reset or multiple pass method. SERC learned that URE disposed of 324 devices and redeployed seven devices during this time period. However, in every instance, the data on the devices was erased by a factory reset or a data wipe using the accepted multiple pass wipe method.

SERC determined that URE was in violation of CIP-007-1 R7.2 for failing to correctly document an acceptable data cleansing method for the redeployment of Cyber Assets in order to prevent unauthorized retrieval of sensitive cyber security or reliability data.

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

SERC determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. While URE had documented an incorrect procedure, it was utilizing acceptable data cleansing methods for the disposal and redeployment of Cyber Assets.

SERC201000479 CIP-007-1 R8

CIP-007-1 R8 provides:

> 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:
>
> R8.1. A document identifying the vulnerability assessment process;
>
> 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;
>
> R8.3. A review of controls for default accounts; and,

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-007-1 R8 has a "Lower" VRF and a "Severe" VSL. .

SERC sent URE a CIP Spot Check Notice. The CIP Spot Check team found that URE had failed to perform a CVA of all of the Cyber Assets within the ESP prior to its compliance date.

SERC learned that URE had a procedure in place that addressed the execution of a CVA as required by CIP-007 R8.1. According to URE, it failed to perform the CVA on approximately 495 Cyber Assets because it thought it had a year following the compliance date to perform the CVA and still be in compliance with the Standard.

SERC determined that URE was in violation of CIP-007-1 R8 for failing to perform an annual CVA on its Cyber Assets located in the ESPs.

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE's failure to perform a CVA on the Cyber Assets, prior to implementation of its cyber security program, in the ESPs increased the risk of weaknesses in the security of the Cyber Assets going undetected. This lack of assessment increased the risk to CCAs being compromised and/or rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS.

SERC200900316 CIP-009-1 R1

The purpose statement of Reliability Standard CIP-009-1 provides in pertinent part: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow

established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-009-1 R1 provides:

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

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

URE self-reported a violation of CIP-009-1 R1 because it did not have recovery plans for all of its CCAs. SERC learned that recovery plans had not been created for four device types. URE's database is used to document all critical and non-critical Cyber Assets and access points to the ESPs pursuant to CIP-005-1 R1.6. Because the device types were not in URE's database, they did not have disaster recovery plans. SERC determined that URE was in violation of CIP-009-1 R1 for failing to create and annually review recovery plan(s).

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

SERC determined that this violation posed a serious and substantial risk to the reliability of the BPS because URE's failure to document recovery plans could have resulted in CCAs not being recovered in a timely fashion, which could lengthen the period of time needed to recover from an incident and reduce BPS reliability. URE did not have recovery plans for four device types for almost two years.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of nine hundred fifty thousand dollars ($950,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE submitted Self-Reports for the violations of CIP-002-1 R3, CIP-004-1 R1, CIP-005-1 R1, CIP-006-1 R1, R3, R4, R5, CIP-007-1 R1, R2, R3, R4, R5, R6, CIP-007-2a R6, and CIP-009-1 R1;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violations, which SERC considered a mitigating factor;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
5. CIP-002-1 R3, CIP-005-1 R1, R2, R3, R4, CIP-006-1 R1, R3, R6, CIP-007-1 R2, R3, R4, R5, R6, R8, and CIP-009-1 R1 posed a serious or substantial risk to the reliability of the BPS, the violations of CIP-002-1 R2, CIP-007-1 R1, and CIP-007-2a R6, posed moderate risks to the reliability of the BPS, and the violations of CIP-003-1 R1, CIP-004-1 R2, R4, CIP-006-1 R4, and R5 posed a minimal risk to the reliability of the BPS;
6. SERC considered that URE's situation stemmed from being unprepared when the CIP requirements at issue became mandatory and enforceable for URE. One of the root causes of URE's CIP program failure was URE's lack of knowledge and identification of CCAs, Cyber Assets and access points. Because of this, the devices were not afforded all of the protections of the applicable CIP Standards;
7. Considering the totality of the circumstances; SERC determined that URE's CIP program failure posed a serious risk to the BPS. URE's procedures often lacked the detail required to achieve compliance with the CIP Standards. Personnel's lack of awareness regarding URE's CIP program and its dependence on manual processes, which were eventually automated, also contributed to the situation. Additionally, URE's lack of knowledge and identification of CCAs, Cyber Assets and access points resulted in the devices not being afforded all of the protections of the applicable CIP Standards. This greatly increased the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS; and

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

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of nine hundred fifty thousand dollars ($950,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plan[6]

SERC200900320 CIP-002-1 R2

URE's Mitigation Plan to address its violation of CIP-002-1 R2[7] was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT002863-1 and was submitted as non-public information to FERC in accordance with FERC orders. A revised Mitigation Plan was submitted to SERC. The revised Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002863 and was submitted as non-public information to FERC.

URE's Mitigation Plan required URE to:

1. Revise the risk based assessment methodology to include a reconciliation of the associated CCAs with the corresponding Critical Assets;
2. Update applicable procedures to ensure that the database maintains the relationships between CCAs and their associated Critical Assets; and
3. Use the database to generate the official Critical Asset list and the CCA list.

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

1. The revised risk based methodology;
2. The applicable updated procedures; and
3. The Critical Asset list and the CCA list.

[6] *See* 18 C.F.R § 39.7(d)(7). Due to the nature and number of violations, as well as the fact that many Mitigation Plans were revised multiple times, SERC approved them only after the full scope of issues was determined.
[7] The Mitigation Plan was submitted listing a violation of CIP-002-1 R3 instead of CIP-002-1 R2. The revised Mitigation Plan corrected this issue.

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

SERC200900297 CIP-002-1 R3

URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT002846 and was submitted as non-public information to FERC on accordance with FERC orders.

URE's Mitigation Plan stated URE had taken the following actions:

1. Updated the database and CCA list;
2. Updated the procedures associated with CCA inventory and the reconciliation of the CCA list;
3. Filed applicable Technical Feasibility Exceptions (TFEs); and
4. Provided additional training addressing the updated procedures.

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

1. The updated database inventory list and the updated CCA list;
2. The updated procedures;
3. The TFEs; and
4. Attendance rosters and training materials

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

SERC201000515 CIP-003-1 R1

URE's Mitigation Plan to address its violation of CIP-003-1 R1 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003722 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Made the cyber security policy readily available to all persons who have access to, or are responsible, for CCAs;
2. Posted signs to notify persons of the availability of the cyber security policy; and
3. Updated the cyber security policy to reflect the requirements of the Standard and trained applicable personnel.

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

1. Documentation confirming that the cyber security policy was readily available to all persons who have access to or are responsible for CCAs;
2. Picture showing that paper copies of the cyber security policy are available; and
3. The updated cyber security policy and attendance rosters.

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

SERC200900321 CIP-004-1 R2

URE's Mitigation Plan to address its violation of CIP-004-1 R2 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT002864 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Revised the procedure and trained the applicable personnel;
2. Provided access to the training record database to the newly assigned manager, who has the responsibility of reviewing training completion status, including providing information to access approvers;
3. Refined the CCA personnel eligibility list to include training completion status;

4. Developed procedure for CCA personnel eligibility list maintenance;
5. Consolidated the seven training modules into one module;
6. Revised other applicable procedures; and
7. Removed individuals from the list.

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

1. The revised procedures and attendance rosters;
2. Attestation designating new manager;
3. Email allowing the manager to access the training record database;
4. The refined CCA personnel eligibility list;
5. The CCA personnel eligibility list maintenance procedure;
6. Documentation confirming the consolidation of the seven training modules;
7. The revised procedures; and
8. List with the individuals removed.

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

SERC200900283 CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT002841 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Removed individuals who no longer required access to CCAs;

2. Updated the procedures associated with physical and electronic access to CCAs, including the development of a check list to be used for personnel no longer requiring access; and
3. Provided additional training regarding duties and compliance with CIP-004 R4.

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

1. Documentation confirming the removal of the individuals from the access lists;
2. The updated procedures; and
3. Attendance rosters and training materials.

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

SERC200900290 CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002842 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Reconfigured the failed firewalls;
2. Validated the ESP inventory;
3. Updated the ESP drawings;
4. Updated the database;
5. Updated existing procedures to address CIP-005 R1;
6. Decommissioned/removed undocumented access points from the ESP;
7. Changed the default community strings on the identified firewalls; and
8. Trained applicable personnel on the updated procedures.

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

1. Documentation confirming the reconfiguration of the firewalls;
2. Documentation confirming the validation of the ESP inventory;
3. The updated ESP drawings;
4. Documentation confirming updating the database;
5. The updated procedures;
6. Documentation confirming the decommissioning/removal of undocumented access points;
7. Documentation confirming the modification to the default community strings; and
8. Attendance rosters and training materials.

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

SERC201000480 CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003720 and was submitted as non-public information to FERC on April 18, 2012 in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Implemented strong procedural and technical controls to ensure authentication of the accessing party at access points as required by R2.4;
2. Developed an additional procedure addressing the need of ports and services;
3. Performed a review of the firewall rules;
4. Reviewed the electronic access lists that had been missed;

5. Added the quarterly review of electronic access lists to the applicable review and maintenance procedure; and
6. Trained employees on the change management program.

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

1. The procedural and technical controls that had been implemented to ensure authentication of the accessing party at access points as required by R2.4;
2. The procedure addressing the need of ports and services;
3. Documentation confirming the review of the firewall rules;
4. The reviewed electronic access lists;
5. The amended review and maintenance procedure; and
6. Attendance rosters and training materials.

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

SERC200900421 CIP-005-1 R3

URE's Mitigation Plan to address its violation of CIP-005-1 R3 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002960 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Configured the access points to log incoming traffic;
2. Verified the classification of firewalls in the monitoring tool;
3. Implemented a new procedure with instructions on adding firewalls to the monitoring tool;
4. Updated the existing monitoring, logging and alerting procedure to include a reference to the new procedure; and

5. Trained the applicable personnel on the new procedure and changes to the existing procedure.

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

1. Documentation confirming the configuration of the access points;
2. Documentation confirming the firewall rule configurations;
3. The new procedure;
4. The updated procedure; and
5. Attendance rosters and training materials.

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

SERC201000483 CIP-005-1 R4

URE's Mitigation Plan to address its violation of CIP-005-1 R4 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003579 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Completed the CVA on its electronic access points; and
2. Updated the applicable procedures to require a CVA to be performed and documented for any new access point to an ESP before it is established in a production environment.

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

1. URE's CVA; and
2. The updated procedures.

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

SERC200900357 CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT002955 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Corrected the PSP drawings;
2. Completed the six-wall borders at the applicable PSPs;
3. Added a procedure detailing visitor access control;
4. Disciplined applicable personnel;
5. Revised the applicable procedures to identify that PSP and ESP changes are addressed by URE's change management process;
6. Afforded the protective measures specified in CIP-007 and CIP-009 to the security access controller system; and
7. Trained the applicable personnel on the new procedure and changes to the existing procedures.

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

1. The updated PSP drawings;
2. Documentation confirming the completion of the six wall borders;
3. The new procedure;
4. Documentation confirming that disciplinary actions were taken;
5. The revised procedures;

6. Documentation verifying that the protective measures specified in CIP-007 and CIP-009 were provided to the security access controller system; and
7. Attendance rosters and training materials.

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

SERC200900393 CIP-006-1 R3

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002957 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Fixed the door controller security system so that it issued alerts;
2. Added window alarm contacts to the applicable windows;
3. Modified the alarm review process to include a peer check for verification;
4. Revised the physical access to CCA sites procedure;
5. Repaired failed equipment;
6. Added the omitted PSP doors to the security system to allow for alarming;
7. Created a maintenance and testing procedure addressing PSP door configuration;
8. Provided additional training to applicable personnel regarding physical security processes and procedures; and
9. Created a procedure to guide the establishment/re-establishment of ESPs.

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

1. Documentation confirming the repair of the door controller security system;

2. Documentation confirming the addition of the window alarm;
3. The modified alarm review process;
4. The revised procedure;
5. Documentation confirming the repair of the failed equipment;
6. The PSP door configuration maintenance and testing procedure;
7. Attendance rosters and training materials; and
8. The establishment/re-establishment of ESPs procedure.

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

SERC201000627 CIP-006-1 R4

URE's Mitigation Plan to address its violation of CIP-006-1 R4 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT004861 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Provided additional training to applicable personnel regarding URE's physical security policy;
2. Posted signs on doors to raise visitor access awareness;
3. Added a procedure detailing visitor access control; and
4. Disciplined involved personnel.

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

1. The attendance rosters and the training materials;
2. Pictures showing signs posted on doors;

3. The new procedure; and
4. Document showing the disciplinary action that was taken.

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

SERC201000486 CIP-006-1 R5

URE's Mitigation Plan to address its violation of CIP-006-1 R5 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003581 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Transferred control of the physical security environment at the affected operations center to a new server; and
2. Updated the procedure to include specific language related to archiving and retaining access logs and trained applicable personnel.

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

1. Change ticket for the transfer of control to the new server;
2. The updated procedure;
3. Attendance rosters and training materials.

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

SERC201000484 CIP-006-1 R6

URE's Mitigation Plan to address its violation of CIP-006-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated

as SERCMIT003580 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Executed and documented the testing of security controls at all existing PSPs; and
2. Updated the physical security procedure to state that PSP security controls will be tested and documented prior to establishing a new PSP or when changing an existing PSP.

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

1. Documentation confirming the testing of the security controls at the PSPs and
2. The updated physical security procedure.

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

SERC200900310 CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002853 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Validate the configurations on the missed devices;
2. Hire a security control testing consultant to update security control procedures and train applicable personnel on the changes; and
3. Implement an automated monitoring tool to detect and document changes to security configurations.

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

1. Documentation confirming the configurations validation;
2. The outside consulting firm contract;
3. The updated security control procedures;
4. Attendance rosters and the training materials;
5. Documentation confirming the implementation of the automated security controls monitoring tool.

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

SERC200900312 CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002855 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Developed an additional procedure that details the process for assessing ports and services including the creation of baselines and their verification;
2. Performed verification of the ports and services;
3. Provided training on change management program; and
4. Removed remnants from the antivirus program.

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

1. The new procedure;

2. Ports and services verification documentation;
3. The change management program training presentation and attendance records;
4. Screen shot that shows that the antivirus program was disabled.

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

SERC200900313 CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002856 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Assessed the missed patches;
2. Reviewed and verified the application inventory;
3. Implemented processes and procedures for inventory maintenance and patch availability monitoring;
4. Updated applicable procedures; and
5. Trained applicable personnel on the new processes and procedures and the updated procedures.

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

1. Documentation confirming the assessment of the missed patches;
2. Documentation confirming the review and the verification of the application inventory;
3. The new processes and procedures addressing inventory maintenance and patch availability monitoring;

4. The updated procedures; and
5. Attendance rosters and training materials.

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

SERC201000688 CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT004863 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Re-installed the antivirus scanner on the identified server;
2. Decommissioned the server that was no longer in production;
3. Added the identified missing devices to the database;
4. Submitted and/or updated the TFEs;
5. Configured the security status monitoring tools to monitor and alert if antivirus software failures occur; and
6. Updated the procedures associated with CIP-007 R4 and trained applicable personnel.

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

1. Documentation confirming the re-installation of the antivirus scanner;
2. Documentation confirming the decommissioning of unnecessary devices;
3. Documentation confirming the addition of the devices to the database;
4. The new and amended TFEs;

5. Documentation confirming the monitoring of antivirus software;
6. Attendance rosters and training materials.

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

SERC200900315 CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002858 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Validated the ESP inventory;
2. Ensured that all Cyber Assets within ESPs have passwords that meet CIP-007 requirements;
3. Decommissioned assets that could not support CIP-compliant passwords;
4. Changed and reissued shared account passwords that were erroneously distributed;
5. Created shared account manual logging processes and trained applicable personnel;
6. Disabled the shared accounts that were not needed; and
7. Updated the policy/procedures to address CIP-007-1 R5.2 and R5.3 and trained applicable personnel.

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

1. Documentation confirming validation of the ESP inventory;
2. Documentation confirming that Cyber Assets within ESPs have passwords that meet CIP-007 requirements;

3. Documentation confirming the decommissioning of assets that could not support CIP compliant passwords;
4. Documentation confirming the change and re-issuance of the shared account passwords;
5. The new shared account manual logging processes;
6. Attendance rosters and training materials;
7. Documentation verifying the disablement of the shared accounts that were not needed;
8. The updated policy and procedures; and
9. Attendance rosters and training materials.

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

SERC200900314 CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002857 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Add the missing devices to the database;
2. Revise the applicable procedures;
3. Update the TFE;
4. Implement a process to reconcile the device lists from database and the monitoring tool semi-annually;
5. Add alerts that monitor the health of the monitoring tool to the network operation center's responsibilities;
6. Train applicable personnel on the monitoring tool configuration and the procedure changes; and

7. Create a new procedure for developing TFEs.

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

1. Documentation confirming the addition of the devices;
2. The revised procedures;
3. The updated TFE;
4. The new process;
5. Documentation confirming the addition of alerts;
6. Attendance rosters and training materials; and
7. The new TFE procedure.

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

SERC201000577 CIP-007-2a R6

URE's Mitigation Plan to address its violation of CIP-007-2a R6 was submitted to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT004812-1 and was submitted as non-public information to FERC in accordance with FERC orders. URE submitted an extension request as a revised Mitigation Plan with a new expected completion date. The extension was granted by SERC.

URE's Mitigation Plan required URE to:

1. Revise the applicable procedures to address application-specific guidance as well as the installation of antivirus patches to the automated monitoring tool;
2. Implement a redundant monitoring tool; and
3. Hold a status meeting regarding the implementation of the monitoring tool.

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

1. The revised procedures;
2. Documentation confirming the occurrence of the status meeting; and
3. Documentation establishing the implementation of the redundant monitoring tool.

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

SERC201000485 CIP-007-1 R7

URE's Mitigation Plan to address its violation of CIP-007-1 R7 was submitted to SERC. The Mitigation Plan was accepted by SERC on and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT004515 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to update the procedure and train applicable personnel.

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

1. The updated procedure; and
2. Attendance rosters and the training materials.

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

SERC201000479 CIP-007-1 R8

URE's Mitigation Plan to address its violation of CIP-007-1 R8 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERCMIT003719 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Completed the CVA on the ESPs; and
2. Updated the applicable procedures to require a CVA to be performed and documented for any new ESP before it is established in a production environment.

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

1. The CVA; and
2. The updated procedures.

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

SERC200900316 CIP-009-1 R1

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted as complete to SERC. The Mitigation Plan was accepted by SERC and approved by NERC. The Mitigation Plan for this violation is designated as SERMIT002859 and was submitted as non-public information to FERC in accordance with FERC orders.

URE completed the following actions detailed in its Mitigation Plan:

1. Updated the procedure for recovery plans to include the missing Cyber Assets;
2. Conducted an exercise using the recovery plans for the missing Cyber Assets;
3. Validated the ESP inventory; and
4. Updated various Cyber Asset procedures to address CIP-009.

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

1. The revised procedure;

2. Recovery drill confirmation memo and presentation;
3. The results of the network scan; and
4. The updated Cyber Asset procedures.

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[8]

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,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2012. The NERC BOTCC approved the Settlement Agreement, including SERC's assessment of a nine hundred fifty thousand dollar ($950,000) 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. URE was cooperative throughout the compliance enforcement process;
2. URE self-reported the initial violations of CIP-002-1 R3, CIP-004-1 R1, CIP-005-1 R1, CIP-006-1 R1, R3, R4, R5CIP-007-1 R1, R2, R3, R4, R5, R6, CIP-007-2a R6, and CIP-009-1 R1;
3. URE had a compliance program at the time of the violations which SERC considered a mitigating factor;
4. There was no evidence of any attempt to conceal a violation nor evidence of intent to do so;

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

5. SERC determined that the violations of CIP-002-1 R3, CIP-005-1 R1, R2, R3, R4, CIP-006-1 R1, R3, R6, CIP-007-1 R2, R3, R4, R5, R6, R8, and CIP-009-1 R1 posed a serious or substantial risk to the reliability of the BPS, the violations of CIP-002-1 R2, CIP-007-1 R1, and CIP-007-2a R6, posed moderate risks to the reliability of the BPS, and the violations of CIP-003-1 R1, CIP-004-1 R2, R4, CIP-006-1 R4, and R5 posed a minimal risk to the reliability of the BPS; and
6. SERC considered that URE's situation stemmed from being unprepared when the CIP requirements at issue became mandatory and enforceable for URE. One of the root causes of URE's CIP program failure was URE's lack of knowledge and identification of CCAs, Cyber Assets and access points. Because of this, the devices were not afforded all of the protections of the applicable CIP Standards;
7. Considering the totality of the circumstances, SERC determined that URE's CIP program failure posed a serious risk to the reliability of the BPS. URE's procedures often lacked the detail required to achieve compliance with the CIP Standards. Personnel's lack of awareness regarding URE's CIP program and its dependence on manual processes, which were eventually automated, also contributed to the situation. Additionally, URE's lack of knowledge and identification of CCAs, Cyber Assets and access points resulted in the devices not being afforded all of the protections of the applicable CIP Standards. This greatly increased the risk of CCAs being compromised and rendered inoperable. Compromised and/or inoperable CCAs could have caused the loss of monitoring and control of the BPS; and
8. 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 nine hundred fifty thousand dollars ($950,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

Information in and certain attachments to the instant NOP include confidential information as defined by the Commission's regulations at 18 C.F.R. Part 388 and orders, as well as NERC Rules of Procedure including the NERC CMEP Appendix 4C to the Rules of Procedure. This includes non-public information

related to certain Reliability Standard violations, certain Regional Entity investigative files, Registered Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be Included as Part of this Notice of Penalty

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

a) Settlement Agreement by and between SERC and URE executed December 20, 2012, included as Attachment a;

   1. SERC's Disposition of Violation: Information Common to Instant Violations, included as Attachment A to the Settlement Agreement;
   2. SERC's Disposition of Violation for CIP-004-1 R4, included as Attachment B to the Settlement Agreement;
   3. SERC's Disposition of Violation for CIP-005-1 R1, included as Attachment C to the Settlement Agreement;
   4. SERC's Disposition of Violation for CIP-002-1 R3, included as Attachment D to the Settlement Agreement;
   5. SERC's Disposition of Violation for CIP-007-1 R1, included as Attachment E to the Settlement Agreement;
   6. SERC's Disposition of Violation for CIP-007-1 R2, included as Attachment F to the Settlement Agreement;
   7. SERC's Disposition of Violation for CIP-007-1 R3, included as Attachment G to the Settlement Agreement;
   8. SERC's Disposition of Violation for CIP-007-1 R6, included as Attachment H to the Settlement Agreement;

9. SERC's Disposition of Violation for CIP-007-1 R5, included as Attachment I to the Settlement Agreement;
10. SERC's Disposition of Violation for CIP-009-1 R1, included as Attachment J to the Settlement Agreement;
11. SERC's Disposition of Violation for CIP-002-1 R2, included as Attachment K to the Settlement Agreement;
12. SERC's Disposition of Violation for CIP-004-1 R2, included as Attachment L to the Settlement Agreement;
13. SERC's Disposition of Violation for CIP-006-1 R1, included as Attachment M to the Settlement Agreement;
14. SERC's Disposition of Violation for CIP-006-1 R3 and R5, included as Attachment N to the Settlement Agreement;
15. SERC's Disposition of Violation for CIP-005-1 R3, included as Attachment O to the Settlement Agreement;
16. SERC's Disposition of Violation for CIP-007-1 R8, included as Attachment P to the Settlement Agreement;
17. SERC's Disposition of Violation for CIP-005-1 R2, included as Attachment Q to the Settlement Agreement;
18. SERC's Disposition of Violation for CIP-005-1 R4, included as Attachment R to the Settlement Agreement;
19. SERC's Disposition of Violation for CIP-006-1 R6, included as Attachment S to the Settlement Agreement;
20. SERC's Disposition of Violation for CIP-007-1 R7, included as Attachment T to the Settlement Agreement;
21. SERC's Disposition of Violation for CIP-006-1 R5, included as Attachment U to the Settlement Agreement;
22. SERC's Disposition of Violation for CIP-003-1 R1, included as Attachment V to the Settlement Agreement;
23. SERC's Disposition of Violation for CIP-007-2a R6 , included as Attachment W to the Settlement Agreement;

24. SERC's Disposition of Violation for CIP-006-1 R4, included as Attachment X to the Settlement Agreement; and
25. SERC's Disposition of Violation for CIP-007-1 R4, included as Attachment Y to the Settlement Agreement.

b) Record documents for the violation of CIP-002-1 R2, included as Attachment b:

1. SERC's source document;
2. URE's Mitigation Plan designated as SERCMIT002863-1;
3. URE's revised Mitigation Plan designated as SERMIT002863; and
4. URE's Certification of Mitigation Plan Completion.

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

1. URE's Self-Report;
2. URE's addendum;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. URE's Mitigation Plan designated as SERCMIT002846; and
7. URE's Certification of Mitigation Plan Completion.

d) Record documents for the violation of CIP-003-1 R1, included as Attachment d:

1. SERC's source document;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as SERCMIT003722; and
4. URE's Certification of Mitigation Plan Completion.

e) Record documents for the violation of CIP-004-1 R2, included as Attachment e:

1. SERC's source document;
2. URE's Mitigation Plan designated as SERCMIT002864; and
3. URE's Certification of Mitigation Plan Completion.

f) Record documents for the violation of CIP-004-1 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. URE's Self-Report;
7. URE's Mitigation Plan designated as SERCMIT002841; and
8. URE's Certification of Mitigation Plan Completion.

g) Record documents for the violation of CIP-005-1 R1, included as Attachment g:

1. URE's Self-Report;
2. URE's addendum;
3. URE's addendum;
4. SERC's source document;
5. URE's addendum;
6. URE's addendum;
7. URE's addendum;
8. URE's Self-Report;
9. URE's Self-Report;
10. URE's Self-Report;
11. URE's Self-Report;
12. URE's Self-Report;
13. URE's Self-Report;
14. URE's Self-Report;
15. URE's Self-Report;
16. URE's Self-Report;
17. URE's Self-Report;

18. URE's Self-Report;
19. URE's Mitigation Plan designated as SERMIT002842; and
20. URE's Certification of Mitigation Plan Completion.

h) Record documents for the violation of CIP-005-1 R2, included as Attachment h:
   1. SERC's source document;
   2. URE's addendum;
   3. URE's Self-Report;
   4. URE's Mitigation Plan designated as SERMIT003720; and
   5. URE's Certification of Mitigation Plan Completion.

i) Record documents for the violation of CIP-005-1 R3, included as Attachment i:
   1. URE's self-report;
   2. URE's source document;
   3. URE's addendum;
   4. URE's addendum;
   5. URE's Mitigation Plan designated as SERCMIT002960; and
   6. URE's Certification of Mitigation Plan Completion.

j) Record documents for the violation of CIP-005-1 R4, included as Attachment j:
   1. URE's source document;
   2. URE's Mitigation Plan designated as SERCMIT003579; and
   3. URE's Certification of Mitigation Plan Completion.

k) Record documents for the violation of CIP-006-1 R1, included as Attachment k:
   1. URE's Self-Report;
   2. URE's Self-Report;
   3. URE's Self-Report;
   4. URE's Self-Report;
   5. SERC's source document;

6. URE's addendum;
7. URE's addendum;
8. URE's Self-Report;
9. URE's Self-Report;
10. URE's Self-Report;
11. URE's Self-Report;
12. URE's Mitigation Plan designated as SERCMIT002955; and
13. URE's Certification of Mitigation Plan Completion.

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

1. URE's Self-Report;
2. URE's addendum;
3. URE's addendum;
4. URE's addendum;
5. URE's Self-Report;
6. URE's Self-Report;
7. URE's Self-Report;
8. URE's Self-Report;
9. URE's Mitigation Plan designated as SERCMIT002957; and
10. URE's Certification of Mitigation Plan Completion.

m) Record documents for the violation of CIP-006-1 R4, included as Attachment m:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Mitigation Plan designated as SERCMIT004861; and
4. URE's Certification of Mitigation Plan Completion.

n) Record documents for the violation of CIP-006-1 R5, included as Attachment n:

1. URE's Self-Report;

2. URE's Mitigation Plan designated as SERCMIT003581; and
3. URE's Certification of Mitigation Plan Completion.

o) Record documents for the violation of CIP-006-1 R6, included as Attachment o:

1. SERC's source document;
2. URE's Mitigation Plan designated as SERCMIT003580; and
3. URE's Certification of Mitigation Plan Completion.

p) Record documents for the violation of CIP-007-1 R1 included as Attachment p:

1. URE's Self-Report;
2. SERC's source document;
3. URE's Mitigation Plan designated as SERMIT002853; and
4. URE's Certification of Mitigation Plan Completion.

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

1. URE's Self-Report;
2. SERC's source document;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Self-Report;
6. URE's Mitigation Plan designated as SERMIT002855; and
7. URE's Certification of Mitigation Plan Completion.

r) Record documents for the violation of CIP-007-1 R3 included as Attachment r:

1. URE's Self-Report;
2. URE's addendum;
3. URE's Self-Report ;
4. URE's Self-Report;
5. URE's Self-Report;
6. URE's Self-Report;

7. URE's Mitigation Plan designated as SERMIT002856; and
8. URE's Certification of Mitigation Plan Completion.

s) Record documents for the violation of CIP-007-1 R4 included as Attachment s:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's Self-Report;
4. URE's Self-Report;
5. URE's Mitigation Plan designated as SERMIT004863; and
6. URE's Certification of Mitigation Plan Completion.

t) Record documents for the violation of CIP-007-1 R5 included as Attachment t:

1. URE's Self-Report;
2. URE's addendum;
3. URE's Self-Report;
4. URE's addendum;
5. URE's Self-Report;
6. URE's Self-Report;
7. URE's Mitigation Plan designated as SERMIT002858; and
8. URE's Certification of Mitigation Plan Completion.

u) Record documents for the violation of CIP-007-1 R6 included as Attachment u:

1. URE's Self-Report;
2. SERC's source document;
3. URE's addendum;
4. URE's Self-Report;
5. URE's Self-Report;
6. URE's Self-Report;
7. URE's Self-Report;

8. URE's Self-Report;
9. URE's Self-Report;
10. URE's Self-Report;
11. URE's Self-Report;
12. URE's Mitigation Plan designated as SERCMIT002857; and
13. URE's Certification of Mitigation Plan Completion.

v) Record documents for the violation of CIP-007-2a R6 included as Attachment v:

1. URE's Self-Report;
2. URE's Self-Report;
3. URE's addendum;
4. URE's addendum1;
5. URE's addendum;
6. URE's addendum;
7. URE's addendum;
8. URE's Mitigation Plan designated as SERCMIT004812-1; and
9. URE's Certification of Mitigation Plan Completion.

w) Record documents for the violation of CIP-007-1 R7 included as Attachment w:

1. SERC's source document;
2. URE's Mitigation Plan designated as SERCMIT004515; and
3. URE's Certification of Mitigation Plan Completion.

x) Record documents for the violation of CIP-007-1 R8 included as Attachment x:

1. SERC's source document;
2. URE's Mitigation Plan designated as SERCMIT00003719; and
3. URE's Certification of Mitigation Plan Completion.

y) Record documents for the violation of CIP-009-1 R1 included as Attachment y:

1. URE's Self-Report;

2. URE's Mitigation Plan designated as SERCMIT002859; and
3. URE's Certification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[10]
A copy of a notice suitable for publication is included in Attachment z.

[10] *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, D.C. 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net John R.Twitchell* VP and Chief Program Officer SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 940-8205 (704) 357-7914 – facsimile jtwitchell@serc1.org Andrea B. Koch* Manager, Compliance Enforcement SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704)940-8219 (704) 357-7914 – facsimile akoch@serc1.org	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Sonia C. Mendonca* Attorney North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile rebecca.michael@nerc.net sonia.mendonca@nerc.net Marisa A. Sifontes* General Counsel Maggie A. Sallah* Senior Counsel SERC Reliability Corporation 2815 Coliseum Centre Drive, Suite 500 Charlotte, NC 28217 (704) 494-7775 (704) 357-7914 – facsimile msifontes@serc1.org msallah@serc1.org *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/ Rebecca J. Michael

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, D.C. 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

Rebecca J. Michael
Associate General Counsel for Corporate and Regulatory Matters
Sonia C. Mendonca
Attorney
North American Electric Reliability Corporation
1325 G Street, N.W.
Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
rebecca.michael@nerc.net
sonia.mendonca@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments