PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 30, 2013

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

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

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because the Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations[3] of CIP-002-1 R3; CIP-003-1 R5; CIP-004-1 R3; CIP-004-1 R4; CIP-005-1 R2; CIP-005-1 R1; CIP-005-1 R4; CIP-007-1 R8; CIP-006-1 R6; CIP-007-1 R2; CIP-007-1 R3; CIP-007-1 R6; CIP-009-1 R2; CIP-007-1 R1; CIP-003-1 R6; CIP-005-1 R5; CIP-006-1 R1; CIP-006-1 R1.8; CIP-006-1 R2; CIP-006-1 R3; CIP-006-1 R4; CIP-007-1 R4; CIP-007-1 R5; CIP-007-1 R7; CIP-007-1 R9; CIP-008-1 R1; CIP-009-1 R1; and CIP-009-1 R4. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred thousand dollars ($100,000), in addition to other remedies and actions to mitigate the

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

[2] *See* 18 C.F.R § 39.7(c)(2).

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

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 SPP2011008732, SPP2011008733, SPP2011008735, SPP2011008736, SPP2011008737, SPP2011008738, SPP2011008739, SPP2011008756, SPP2011008747, SPP2011008749, SPP2011008751, SPP2011008754, SPP2011008761, SPP2011008748, SPP2011008734, SPP2011008740, SPP2011008742, SPP2011008743, SPP2011008744, SPP2011008745, SPP2011008746, SPP2011008752, SPP2011008753, SPP2011008755, SPP2011008757, SPP2011008759, SPP2011008760, and SPP2011008762 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 5, 2013, by and between SPP RE and URE, which is included as Attachment a. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2013), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Southwest Power Pool Regional Entity	Unidentified Registered Entity	NOC-1792	SPP2011008732	CIP-002-1	R3; R3.2	Lower	$100,000
			SPP2011008733	CIP-003-1	R5; R5.1	Lower	
			SPP2011008735	CIP-004-1	R3; R3.1	Medium	
			SPP2011008736		R4	Lower	
			SPP2011008737	CIP-005-1	R2; R2.1, R2.2, R2.4	Medium	
			SPP2011008738		R1	Medium	

Southwest Power Pool Regional Entity	Unidentified Registered Entity	NOC-1792	SPP2011008739	CIP-005-1	R4; R4.1, R4.2, R4.3, R4.4, R4.5	Medium	$100,000
			SPP2011008756	CIP-007-1	R8; R8.1, R8.2, R8.4	Lower	
			SPP2011008747	CIP-006-1	R6	Medium	
			SPP2011008749	CIP-007-1	R2; R2.1, R2.2	Medium	
			SPP2011008751		R3	Lower	
			SPP2011008754		R6; R6.5	Lower	
			SPP2011008761	CIP-009-1	R2	Lower	
			SPP2011008748	CIP-007-1	R1; R1.1	Medium	
			SPP2011008734	CIP-003-1	R6	Lower	
			SPP2011008740	CIP-005-1	R5.1; R5.3	Lower	
			SPP2011008742	CIP-006-1	R1.1; R1.2; R1.4; R1.6	Medium	
			SPP2011008743		R1.8	Medium	
			SPP2011008744		R2	Medium	

Southwest Power Pool Regional Entity	Unidentified Registered Entity	NOC-1792	SPP2011008745	CIP-006-1	R3	Medium	$100,000
			SPP2011008746		R4	Lower	
			SPP2011008752	CIP-007-1	R4	Medium	
			SPP2011008753		R5	Lower	
			SPP2011008755		R7	Lower	
			SPP2011008757		R9	Lower	
			SPP2011008759	CIP-008-1	R1.1; R1.3; R1.4; R1.5; R1.6	Lower	
			SPP2011008760	CIP-009-1	R1	Medium	
			SPP2011008762		R4	Lower	

CIP-002-1 R3

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

> NERC Standards CIP-002 through CIP-009 provide a cyber security framework for the identification and protection of Critical Cyber Assets to support reliable operation of the Bulk Electric System.
>
> These standards recognize the differing roles of each entity in the operation of the Bulk ElectricSystem, the criticality and vulnerability of the assets needed to manage Bulk Electric System reliability, and the risks to which they are exposed. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Business and operational demands for managing and maintaining a reliable Bulk Electric System increasingly rely on Cyber Assets supporting critical reliability functions and processes to communicate with each other, across functions and organizations, for services and data. This results in increased risks to these Cyber Assets.

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

CIP-002-1 R3 provides:

R3. Critical Cyber Asset Identification — Using the list of Critical Assets developed pursuant to Requirement R2, the Responsible Entity shall develop a list of associated Critical Cyber Assets essential to the operation of the Critical Asset. Examples at control centers and backup control centers include systems and facilities at master and remote sites that provide monitoring and control, automatic generation control, real-time power system modeling, and real-time interutility data exchange. The Responsible Entity shall review this list at least annually, and update it as necessary. For the purpose of Standard CIP-002, Critical Cyber Assets are further qualified to be those having at least one of the following characteristics:

***

R3.2. The Cyber Asset uses a routable protocol within a control center; or,

***

CIP-002-1 R3.2 has a "Lower" Violation Risk Factor (VRF) [4] and a "Severe" Violation Severity Level (VSL).

During a Compliance Audit, SPP RE determined that URE failed to identify certain relays, that use routable protocol to transmit relay data to the control center, located in a substation and a generator control house (collectively, the facility), as Critical Cyber Assets (CCAs) in its CCA list, as determined by its Risk Based Assessment Methodology (RBAM). The affected relays connect serially to communication processors that communicate using routable protocol through the network switches to

[4] Except where a subrequirement is specifically referenced in this section, SPP RE assessed the VRF at the requirement level.

URE's control center Supervisory Control and Data Acquisition (SCADA) and energy management system (EMS) systems.

SPP RE determined the duration of the violation to be the date the Standard became mandatory and enforceable on URE until URE revised its CCA list to include the affected relays.

SPP RE determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, the security afforded to the CCAs at issue was diminished due to URE's concurrent violations of CIP-005-1 R1 and CIP-006-1 R4. URE's violation of CIP-005-1 increased the risk associated with the instant violation because URE was unaware of what users and information were passing through the electronic security perimeter (ESP) access points. URE's CIP-006-1 violations further increase the risk associated with the instant violation because the physical security perimeters (PSPs) at the facility were vulnerable to unauthorized entry. The risk to the reliability of the BPS was mitigated by the following factors. The relays at issue reside within ESPs and PSPs that were established at the substation pursuant to URE's efforts to comply with CIP-005-1 and CIP-006-1. URE's facilities operate at relatively low voltage levels. URE has a small peak load. There are only a few interconnections on the URE system (at a few substations). The facility's generation capacity is also small.

CIP-003-1 R5

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 R5 provides in pertinent part:

> R5. Access Control — The Responsible Entity shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> > R5.1. The Responsible Entity shall maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.

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

During the Compliance Audit, SPP RE determined that two of URE's groups failed to provide evidence of a documented or implemented program for managing access to protected CCA information, in

violation of CIP-003-1 R5. In addition, URE did not have a list of designated personnel who are responsible for authorizing physical access to protected information, in violation of CIP-003-1 R5.1. URE was storing hard copies of CCA information in unsecured boxes in its primary control center (PCC) where personnel without authorized access to the CCA information could access the CCA information. URE did not have evidence that the personnel with authorized physical access to the PCC were granted access to the CCA information located in the unsecured boxes in the PCC.

SPP RE determined the duration of the violation to be from July 1, 2009, the date the Standard became mandatory and enforceable on URE through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not implementing an access management program for certain groups and by storing CCA information in an unsecure location, URE failed to limit employee and contractor access to CCA information. Accordingly, sensitive information related to CCAs could have been compromised, thereby leaving URE's CCAs and Critical Assets unprotected and at risk. The risk to the reliability of the BPS was mitigated by the following factors. URE did have controls in place for authorizing electronic and physical access to the URE Critical Assets. Even though URE did not specifically designate an employee responsible for authorizing physical access to CCA information, it did designate URE employees with authorized physical access to both the PCC and generation facilities which house URE's CCA information.

CIP-004-1 R3

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 R3 provides in pertinent part:

> R3. Personnel Risk Assessment —The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access. A personnel risk assessment shall be conducted pursuant to that program within thirty days of such personnel being granted such access. Such program shall at a minimum include:

> R3.1. The Responsible Entity shall ensure that each assessment conducted include, at least, identity verification (e.g., Social Security Number verification in the U.S.) and seven-year criminal check. The Responsible Entity may conduct more detailed reviews, as permitted by law and subject to existing collective bargaining unit agreements, depending upon the criticality of the position.

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

During a Spot Check, URE failed to provide evidence that three percent of randomly sampled personnel with authorized electronic and unescorted physical access to URE CCAs had received a personnel risk assessment (PRA) that included identity verification and a seven-year criminal background check as required by CIP-003-1 R3.1.

During the Compliance Audit, SPP RE determined that URE failed to perform identity verifications for a few contractors who were granted physical access to URE's CCAs. Furthermore, URE did not have evidence that a seven-year criminal background check was performed for one employee who was granted access to CCAs.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE has a documented PRA program that addresses federal, state, and local laws, in addition to the CIP Reliability Standards. The URE PRA program requires a social security trace (identity verification) for all of its employees. URE's PRAs consistently included identity verification, statewide criminal history, county criminal searches, education verification, employment verification, professional certification verification, and reviewed driving records for the past three years for each employee. URE provided the missing PRA information for the affected employees, and the background checks for these employees came back clean. Also, the contractors who did not have PRAs with identity verifications on file were maintenance contractors who only had physical access to the PSP that contained a non-critical server which was enclosed in a locked cabinet. The contractors did not have electronic access to the CCAs at any time, and the contractors had received the mandatory cyber security training.

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 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that URE failed to maintain its list(s) of personnel with authorized cyber or authorized unescorted physical access to CCAs properly. URE's list of personnel with authorized access to CCAs did not include the specific electronic access rights granted to each individual. In addition, URE's maintained list of personnel and contractors approved for authorized unescorted physical access to CCAs did not list all personnel granted unescorted physical and/or electronic access to CCAs. Finally, URE did not provide evidence that the authorized staff had fully reviewed the list of its personnel who have physical and electronic access to CCAs on a quarterly basis.

There were various discrepancies between the list used for tracking specific access rights by individual and access point (List 1), another access list (List 2), and a badge holder access to logical devices list (List 3). Such discrepancies included: 1) an employee with access only to the control room on List 1 had access to the control room and the relay room but was not on the other two lists; and 2) an employee was listed on List 1 but not the other two lists; however, upon further review, URE discovered that the employee had retired and should not have been on the list.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, because URE did not include specific electronic access rights on its list of personnel with authorized access to CCAs and was not maintaining a comprehensive list of all personnel granted unescorted physical and/or electronic access to its CCAs, the violation created a risk of unauthorized access to CCAs. The risk to the reliability of the BPS was mitigated by the following factors. Although URE's list of personnel with authorized access to CCAs did not include specific electronic access rights, URE's policy was that access to its CCAs was only granted to employees and contractors on an as-needed basis, providing a layer of review by authorized personnel. URE timely revoked access of any individuals that were terminated, resigned, or no longer needed access to URE's CCAs.

CIP-005-1 R2

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 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> > R2.1. 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.

***

> R2.4. 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.
>
> ***
>
> R2.6. 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 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that URE had a violation of CIP-005-1 R2, including R2.1, R2.2, and R2.4. URE was not able to provide documented organizational processes and/or technical procedures for control of electronic access to the facility's electronic access points as required by CIP-005-1 R2.

URE had a violation of R2.1 for failing to use an access control model that denies access by default. Specifically, URE failed to have an implemented access control list for the switches at the facility. By not having a list for the switches, URE was unaware if the switches were denying electronic access by default.

URE had a violation of R2.2 because certain firewall rules at the facility that were not required for operations or for monitoring Cyber Assets within the ESP had not been disabled or removed, thereby leaving the associated ports open. Specifically, certain firewall rules were not removed or disabled when no longer needed in both the PCC and BCC. Furthermore, the switches deployed as electronic access control systems at the facility were not capable of implementing access control lists to restrict pass-through traffic, and no Technical Feasibility Exception (TFE) had been requested. One of these switches still had telnet enabled which allowed URE Cyber Assets to connect to remote computers over its transmission control protocol/Internet protocol network.

URE had a violation of R2.4 for failing to have strong technical controls to ensure the authenticity of an accessing party attempting to access its ESP using external interactive access. Specifically, URE did not consider its virtual private network (VPN) tunnel to be interactive access to its ESP. Therefore, URE was not properly authenticating accessing parties to the ESP. Any interactive access, including access

that is initiated from a separate ESP, must be authenticated by the ESP and is, therefore subject to CIP-005-1 R2.4. URE had not requested a TFE for its VPN tunnel. In addition, interactive access to the replication service implemented on the Inter Control Communication Protocol (ICCP) servers was not authenticated at the electronic access point as required for users accessing the system from outside the ESP.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not implementing a process or procedure for control of electronic access points to the ESP, the CCAs within the ESP could be exposed to an unauthorized security breach. Furthermore, URE was not monitoring Cyber Assets within the ESP at the facility and therefore was not disabling firewall rules in a timely manner. This left the associated ports open, creating a risk that the CCAs essential for the operation of the bulk BPS could be vulnerable to a cyber attack. URE also did not remove or disable firewall rules in its PCC and backup control center (BCC), which are located at the facility. This created an additional risk because the associated ports remained open, leaving the potential that the associated CCAs could be vulnerable to unauthorized access. In addition, by not authenticating virtual private network access from ESP to ESP, URE left access points open to unauthorized access and at risk.

The risk to the reliability of the BPS was mitigated by the following factors. URE had a procedure in place for control of electronic access points for its PCC which decreased potential for successful attacks against a number of its CCAs. Each individual user had to be defined in the firewall rule set and in the Internet Information Services on the web servers for the SCADA program to work. In addition, access lists were being maintained to ensure only authorized individuals were using the SCADA. By performing an additional manual authorization of access to its SCADA system, URE was providing additional protections of access to CCAs that are critical to protecting the BPS.

CIP-005-1 R1

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).

***

R1.3. 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).

***

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

During the Compliance Audit, SPP RE determined that URE was in violation of CIP-005-1 R1, including R1.1, R1.3, R1.5, and R1.6. With respect to CIP-005-1 R1 and R1.1, URE had not identified electronic access points in the facility ESP. Specifically, there were a number of serial and/or Ethernet link devices installed in the two networks where it was unclear whether or not the end-nodes were additional Cyber Assets. In one instance, the serial and/or Ethernet link devices were connected to an Ethernet port and there was not an electronic access point defined for the data path exiting the ESP. In addition, there were two fiber-optic transceiver/modem devices and remote I/O module that were not documented as to whether or not they were electronic access points.

URE had a violation of CIP-005-1 R1.3 because a VPN tunnel between the core SCADA network at the PCC and the similar network at the BCC terminates at the core firewall pair and should be identified as electronic access points because they are end points of communication links between two ESPs. Neither firewall was identified as an electronic access point, therefore violating R1.3.

URE had a violation of CIP-005-1 R1.5 because it failed to afford the protective measures of CIP-007-1 R4, R5.1.2, and R5.3.3 to Cyber Assets that affect URE's access control and monitoring systems. Anti-virus and other malware prevention tools were not installed on all electronic access control and monitoring systems as required by CIP-007-1 R4 and no TFE was requested, where infeasible. A historical audit trail of individual user account access activity was not being captured and maintained because direct access to the switches services, which are acting as electronic access control and monitoring systems at the affected substation control house, were not being logged as required by CIP-007-1 R5.1.2. Passwords were not being changed at least annually on the firewalls serving as electronic access control and monitoring systems at the PCC and BCC as required by CIP-007-1 R5.3.3.

URE had a violation of CIP-005-1 R1.6 because it failed to account for two Cyber Assets within the ESP on its ESP diagram. Specifically, the second GPS satellite receiver at the PCC was not documented on either the ESP diagram or URE's approved list of CCAs. Although the satellite clock is on its own network, it is connected to the ESP networks and is also within URE's defined ESP. Therefore, it should have been depicted on both the diagram and the CCA list. Additionally, the end-nodes that were referenced in R1 at the facility should have been documented as Cyber Assets within the ESP.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's CCAs were potentially exposed to a cyber security breach because the points were not being monitored. In addition, URE was unable to define the boundary of its ESP, and URE left two ESPs vulnerable to a cyber security breach. This violation rendered URE's system more vulnerable to cyber attack. The failure to change a substantial number of passwords on at least an annual basis leaves cyber systems vulnerable to possible attempts from unauthorized parties outside the ESP to access remotely systems inside the ESP.

The risk to the reliability of the BPS was mitigated by the following factors. URE's manual logging reviews would have alerted URE personnel to the presence of repeated unauthorized access attempts occurring regularly over a period of time. The Cyber Assets that had not been identified were located within URE's defined ESPs. URE personnel utilize a manual review process to monitor electronic access

at both the PCC and BCC. The URE Epicenter system captures logged events at the facility and sends alerts to the network infrastructure distribution list that includes non-management staff with authorized administrative privileges for investigation if a bad username or bad password is used to try to gain access to the URE system. URE's electronic access and security plan defined a process for granting access to electronic access controls that included employees requesting access via the helpdesk and requiring the supervisor of EMS maintenance to give final approval of the request.

CIP-005-1 R4 and CIP-007-1 R8

CIP-005-1 R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> > R4.1. 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.

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 R8 provides in pertinent part:

> R8. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of all Cyber Assets within the Electronic Security Perimeter at least annually. The vulnerability assessment shall include, at a minimum, the following:
>
> R8.1. 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-005-1 R4 has a "Medium" VRF and CIP-007-1 R8 has a "Lower" VRF.

During the Compliance Audit, SPP RE determined that URE had a violation of R4 for failing to perform a vulnerability assessment against the Cyber Assets in the facility. Specifically, URE was unable to provide a documented vulnerability process for the Cyber Assets and electronic access control and monitoring systems in the facility, in violation of CIP-005-1 R4.1. URE's PCC vulnerability assessment did not identify the enabled ports and services and did not have a list of enabled ports and services compared against the baseline to verify that only ports and services required for operations at these access points are enabled, in violation of CIP-005-1 R4.2. URE also did not review the identified Cyber Assets from the network map per scan to determine if there was any direct connectivity to networks outside of the ESP being assessed, in violation of CIP-005-1 R4.3. URE was unable to provide evidence demonstrating that the community strings[5] were reviewed as part of the PCC vulnerability assessment, in violation of CIP-005-1 R4.4. URE was in violation of CIP-005-1 R4.5 because there was no documentation of a vulnerability assessment performed against the Cyber Assets at the facility.

[5] Community strings are similar to a user identification or password that allows access to a router's or other device's statistics.

Therefore, URE did not prepare an action plan to remediate or mitigate vulnerabilities identified in the assessment.

URE's violation of CIP-007-1 R8 is similar in nature to URE's violation of CIP-005-1 R4. At the Compliance Audit, URE provided the same evidence for its vulnerability assessment. Therefore, URE also has a violation of CIP-007-1 R8, R8.1, R.8.2, and R8.4. URE had not performed a vulnerability assessment against the Cyber Assets in the facility, in violation of CIP-007-1 R8. Specifically, URE was in violation of R8.1 because it could not provide a documented vulnerability process for the Cyber Assets and electronic access control and monitoring (EACM) systems in the facility. URE was in violation of CIP-007-1 R8.2 because its PCC vulnerability assessment did not identify the enabled ports and services and did not have a list of enabled ports and services compared against the baseline to verify that only ports and services required for operations at these access points are enabled. URE was also in violation of CIP-007-1 R8.4 because there was no documentation of a vulnerability assessment performed against the Cyber Assets at the facility. Therefore, URE did not prepare an action plan to remediate or mitigate vulnerabilities identified in the assessment.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, because URE did not perform a vulnerability assessment on its Cyber Assets and electronic access points at the facility, there was not reasonable assurance that the ESP(s) of the facility were secure. URE had not formally documented its vulnerability process for the facility, creating the risk that if a vulnerability assessment had been performed, it would not be performed thoroughly and consistently. The risk to the reliability of the BPS was mitigated by the following factors. URE had performed vulnerability assessments of its PCC since it was required. URE created corrective action plans from the vulnerability assessments and mitigated the vulnerabilities that were identified in the assessments. The PCC is the core of the system. Therefore, by identifying and mitigating vulnerabilities found in the assessment, it was protecting the URE SCADA system and CCAs and Cyber Assets within the PCC's defined ESP. URE's facilities operate at relatively low voltages levels. URE's peak load in the summer was low. There are only a small number of interconnections on the URE system, and these interconnections are at low level. The facility has a small generation capacity, which is not substantial to the BPS in this area.

CIP-006-1 R6

The purpose statement of Reliability Standard CIP-006-1 R6 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 R6 provides:

> R6. Maintenance and Testing — The Responsible Entity shall implement 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.

During the Compliance Audit, SPP RE determined that URE failed to demonstrate that its testing program for physical security systems had been implemented. Specifically, URE was unable to provide evidence that any of the physical security systems had undergone a testing and maintenance inspection for almost three years and seven months.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not implementing a program for testing and maintenance of its physical security systems, URE left potential failures of its Access Control and Monitoring system (ACAM) system unidentified, presenting potential risk of unauthorized physical access to its CCAs. The risk to reliability of the BPS was mitigated by the following factors. The URE PCC is staffed 24 hours a day, seven days a week by operations personnel, and the BCC resided behind a guarded PSP that was stationed and monitored 24 hours a day, seven days by closed circuit television via the URE security desk. Therefore, even if URE had suffered a failure of its ACAM access control equipment, any unauthorized physical access to CCAs would have been detected by URE personnel.

Despite the failure to implement maintenance and testing activities on its ACAM, URE attested that there had been no failures of its ACAM equipment.

CIP-007-1 R2

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 R2 provides in pertinent part:

> 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).

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

During the Compliance Audit, SPP RE determined that URE failed to document ports and services baselines for any of the in-scope CCAs located at the facility. Because URE did not have a documented baseline to show which ports and services were required for normal and emergency operations, URE could not demonstrate that only the required ports and services had been enabled as required by R2.

URE has a violation of CIP-007-1 R2.1 because its documented baseline for its ports and services that serve the SCADA/EMS system in the PCC did not have justification for operational need. URE's process is to perform an initial scan of the system when it is delivered by its SCADA/EMS vendor. However, URE did not perform a review of the ports and services the vendor left enabled to see if there was an operational need for those ports and services.

URE has a violation of CIP-007-1 R2.2 because unneeded ports and services had not been disabled for the Cyber Assets at the facility, and URE had not requested a TFE.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. By leaving ports and services enabled that should have been disabled, the URE system is at risk for an unauthorized individual with potential malicious intent to be able to gain access to URE's CCAs. The risk to the reliability of the BPS was mitigated by the fact that URE had controls and procedures in place that were operational during the period of the violation. Therefore, upon discovery of enabled ports that should be disabled, URE personnel submitted a change control form to the appropriate URE personnel and the ports were promptly disabled.

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 "Severe" VSL.

During the Compliance Audit, SPP RE determined that URE failed to provide evidence that a patch management program had been implemented for the workstation in the substation control house. No patches had been assessed for applicability or installed on the substation control house workstation.

URE was in violation of CIP-007-1 R3.1 because only a specific company's patches were being assessed in the PCC. As a result, URE could not demonstrate that all patches in the PCC are evaluated for applicability within the required 30 days. URE was also in violation of CIP-007-1 R3.2 because URE could not provide compensating measures for not installing the patches and it had not requested a TFE for patches that URE or its vendors determined could not be installed.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, by not having a patch management program to monitor and assess the security patches for the workstation in the substation control house, software essential to the viability of URE's CCAs could be compromised. Because the patches at the substation control house were not assessed or monitored, CCAs were left vulnerable to potential cyber security threats and/or attack by unauthorized individuals with malicious intent.

At the time of the violations, URE's security patch notification process, unrelated to the specific company mentioned above, relied on emails from vendors notifying URE that a patch was available. By not assessing the patches' applicability within the required 30 days, URE had out-of-date patches on its system and created the potential that unauthorized electronic access to its CCAs could occur. Additionally, by not requesting a TFE for patches that were unable to be installed, URE was unaware if there were mitigating measures that could have been applied to its system for additional protection even though those particular two patches were unable to be installed.

The risk to the reliability of the BPS was mitigated by the following factors. The facility has a small generation capacity. Additionally, although all PCC system patches were not being assessed within 30 days, URE did identify and assess both a programming language and computing platform and firmware patches during the PCC annual vulnerability assessment. Therefore, the patches were being evaluated. URE was also implementing all patch updates of the specific company mentioned above on its system on a monthly basis, providing a level of protection to both its electric security system and its CCAs. The specific company's patch updates accounted for at least 89% of the required updates to the URE system. No cyber security event had occurred on the URE system.

CIP-007-1 R6

CIP-007-1 R6 provides in pertinent part:

> R6. Security Status Monitoring — The Responsible Entity shall ensure that all Cyber Assets within the Electronic Security Perimeter, as technically feasible, implement automated tools or organizational process controls to monitor system events that are related to cyber security.
>
> ***
>
> R6.5. 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.

During the Compliance Audit, SPP RE determined that URE had a violation of CIP-007-1 R6, including R6.5. Specifically, not all of URE's in-scope Cyber Assets were capable of generating logs, and URE had not requested a TFE for these Cyber Assets. The affected CCAs were communication processors in the facility.

URE was in violation of CIP-007-1 R6.5 because it failed to maintain records of all system log reviews. The SCADA/EMS support team reviews the EMS application logs as part of their daily system checks, but does not keep a record of the log review. Additionally, information technology (IT) staff failed to provide a record of its review of the domain controller logs or the Intrusion Detection/Prevention System logs.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE did not have physical security controls in place for the facility. Therefore, although the communication processors were not capable of generating logs as required by CIP-007-1 R6, they were also not afforded physical protections of the CIP Reliability Standards. URE's failure to implement security controls could allow unauthorized access to the communications processors, leaving them vulnerable to a cyber security attack. The risk to the reliability of the BPS was mitigated by the following factors. URE was reviewing logs of its system for potential security threats, although the reviews of the system logs were documented inconsistently.

The facility has a small generating capacity of. Finally, URE has not experienced any reportable cyber security incidents on its system during the compliance reporting period.

CIP-009-1 R2

The purpose statement of Reliability Standard CIP-009-1 provides: "Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."
CIP-009-1 R2 provides: "R2. Exercises — The recovery plan(s) shall be exercised at least annually. An exercise of the recovery plan(s) can range from a paper drill, to a full operational exercise, to recovery from an actual incident."

CIP-009-1 R2 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that one of URE's groups was unable to provide evidence that the group exercised its CCA recovery plan for two consecutive years, in violation of CIP-009-1 R2.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Employees from the group had completed the mandatory training on the handling of CCAs. URE provided evidence that for two other groups, it had a recovery plan in place and conducted successful training on their respective recovery plans.

CIP-007-1 R1

CIP-007-1 R1 provides in pertinent part:

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

> R1.1. 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.

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

During the Compliance Audit, SPP RE determined that URE failed to provide evidence that the required cyber security testing was being performed on all in-scope Cyber Assets at the facility as required by CIP-007-1 R1. Additionally, URE could not provide documented cyber security test procedures for the in-scope Cyber Assets at the facility as required by CIP-007-1 R1.1.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of cyber security test procedures could have resulted in a failure to detect and prevent potentially harmful modifications to URE's Cyber Assets at the facility. Harmful modifications could, in turn, introduce vulnerabilities to URE's CCAs in the facility and could have negatively impacted the normal operation of the BPS. The risk to the reliability of the BPS was mitigated by the following factors. Although URE did not have cyber security testing procedures for the in-scope Cyber Assets at the facility, URE's facilities operate at relatively low voltage levels. Also, URE's peak load is low. There are only a few interconnections on the URE system, and these interconnections are at the low level. The facility generation capacity is small.

CIP-003-1 R6

CIP-003-1 R6 provides:

> R6. Change Control and Configuration Management — The Responsible Entity shall establish and document a process of change control and configuration management for adding, modifying, replacing, or removing Critical Cyber Asset hardware or software, and implement supporting configuration management activities to identify, control and document all entity or vendor related changes to hardware and software components of Critical Cyber Assets pursuant to the change control process.

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

SPP RE discovered that URE had a violation of CIP-003-1 R6 because URE's Change Control and Configuration Management (CCCM) documentation was deficient.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's lack of entity-wide CCCM could lead to installation of software and hardware that could be harmful to the CCAs essential for the operation of the BPS. Furthermore, URE's failure to have a formal CCCM procedure could result in exposing Cyber Assets to vulnerability when making modifications to its hardware, software, or security configurations. The risk to the reliability of the BPS was mitigated by the following factors. URE's required a change form to be completed prior to changes being made to any CCAs. This form provided a step-by-step process for applying the changes and was approved by senior management. In addition, all vendor-applied configuration changes or software updates were documented using the change control form. Finally, no changes were made to any CCA hardware or software URE during the pendency of the violation.

CIP-005-1 R5

CIP-005-1 R5 provides in pertinent part:

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

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

During the Compliance Audit, SPP RE determined that URE failed to review at least annually the documentation related to configuration of the ports and services required for operations and for monitoring of the control center Cyber Assets within the ESP, in violation of CIP-005-1 R5.1. Additionally, URE failed to retain, for the required minimum of 90 days, all log information available from switches that grant electronic access to facility, in violation of CIP-005-1 R5.3.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had implemented procedures that afforded the protections of the CIP Reliability Standards for its PCC and BCC. URE was manually reviewing its access logs at both the PCC and the BCC and implemented a process for reporting unusual activity on its system. Finally, no cyber security events have occurred on the URE system during the pendency of the violation.

CIP-006-1 R1

CIP-006-1 R1 provides in pertinent part:

The Responsible Entity shall comply with the following requirements of Standard CIP-006:

> 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.

***

R1.4. 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.

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

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL. URE

During the Compliance Audit, SPP RE determined that URE failed to have its BCC fully enclosed within a defined six-wall boundary, in violation of R1.1.

Further, URE failed to maintain documentation reflecting all physical access points into the PSP and failed to document the controls at all access points, in violation of R1.2.

In addition, URE failed to provide a documented procedure for responding to the loss of the physical access control system or a physical access control system component, in violation of R1.4.

Finally, URE failed to designate the main gate to a facility as a PSP access control point. There was no process for manually logging the actual time of a visitor's entrance and exit from the facility's PSPs, in violation of R1.6.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Access to the plant control room and the BCC was only granted to authorized individuals using card readers or keys. The card readers and keys were strictly controlled by the facility's supervisor of operations and only issued to authorized URE personnel. The grounds of the facility that contain the PSPs were fenced and have two guard stations that are staffed with URE security personnel at all times. URE personnel and visitors must sign in at the guard stations prior to entering the facility and the PSP. The visitors had to be logged in at the facility gate and escorted by URE personnel who had access to the PSP. Visitors were given badges with assigned numbers to identify the visitors uniquely. The badges did not give the visitors access to any of URE's secured areas. The visitors' badges were tracked through the card reader system when scanned at each access point.

CIP-006-1 R1

CIP-006-1 R1 provides in pertinent part:

> The Responsible Entity shall comply with the following requirements of Standard CIP-006:
>
> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.8. Cyber Assets used in the access control and monitoring of the Physical Security Perimeter(s) shall be afforded the protective measures specified in Standard CIP-003, Standard CIP-004 Requirement R3, Standard CIP-005 Requirements R2 and R3, Standard CIP-006 Requirement R2 and R3, Standard CIP-007, Standard CIP-008 and Standard CIP-009.

CIP-006-1 R1 has a "Medium" VRF and a "Severe" VSL. URE

SPP RE determined that URE was in violation of CIP-007 R1, R3, R4, and R8. URE failed to: 1) provide documented test procedures or test results for its Physical Access Control Systems (PACS), in violation of R1; 2) install server service pack that is applicable to its PACS systems due to technical feasibility issues, in violation of R3; 3) have a process for testing the updated signature files prior to installation of anti-virus software on the PACS, in violation of R4; and 4) perform vulnerability assessments of components of the PACS, with the exception of one server.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE was unable to ensure that its Cyber Assets that secure the access points into its PSP were working and able to protect against unauthorized access. URE created an environment of insufficient security and potential malfunctions because it did not ensure that the anti-virus software would work on its system. URE was unaware of any systems or components associated with its PACS that were at risk and vulnerable, and therefore could not prepare a corrective action plan to mitigate any vulnerabilities that may have been found. The risk to the reliability of the BPS was mitigated by the following factors. URE had a cyber security protection of the PACS document that included procedures for monitoring electronic access, defining URE's PSP, PSP

monitoring. URE uses, as part of its PACS, software that monitors physical access points at all times and also receives notifications by alarm if unauthorized access occurred at one of URE's defined access points. The workstations using this software were protected against unauthorized physical access because restricted access is granted only to the human resources department. The workstations are located inside a locked office when URE personnel are not present. URE uses a system that sounds an alarm if a door to a secured area is either forced open or held open. An authorization code must be entered to silence the alarm, and only authorized URE personnel know the code.

CIP-006-1 R2

CIP-006-1 R2 provides:

> R2. Physical Access Controls — The Responsible Entity shall document and implement the operational and procedural controls to manage physical access at all access points to the Physical Security Perimeter(s) twenty-four hours a day, seven days a week. The Responsible Entity shall implement one or more of the following physical access methods:
>
> > R2.1. Card Key: A means of electronic access where the access rights of the card holder are predefined in a computer database. Access rights may differ from one perimeter to another.
> >
> > R2.2. Special Locks: These include, but are not limited to, locks with "restricted key" systems, magnetic locks that can be operated remotely, and "man-trap" systems.
> >
> > R2.3. Security Personnel: Personnel responsible for controlling physical access who may reside on-site or at a monitoring station.
> >
> > R2.4. Other Authentication Devices: Biometric, keypad, token, or other equivalent devices that control physical access to the Critical Cyber Assets.

CIP-006-1 R2 has a "Medium" VRF and a "Severe" VSL.

SPP RE determined that URE failed to have a documented process for managing physical access through the double doors giving access to a generating plant relay room PSP. URE did not have a documented process for unlocking the padlock on the door, in violation of CIP-006-1 R2.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The double doors at issue had not been opened for a long period of time, and only limited URE personnel had access to the keys that could open the padlock. Physical inventory of the keys was taken every year, and a call to the supervisor of compliance is required prior to utilizing a key. URE utilizes card keys, restricted key systems, security personnel, and keypads to manage physical access to its access points to the PSP at all times.

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 "Medium" VRF and a "Severe" VSL.

SPP RE determined that URE failed to monitor physical access to all access control points to its PSPs, in violation of CIP-006-1 R3.1 and R3.2. The double glass doors to the BCC in a URE facility did not have contact alarms, and the doors were not easily observable by operators in the generating plant control room. Additionally, the double doors to the generating plant relay room did not have contact alarms and were not easily observable by URE personnel. Finally, the doors into two substation control houses had contact alarms, but URE could not provide evidence of where the contact alarms were being sent. Therefore, URE personnel were not being notified by the alarms.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The facility at issue resides behind a guarded PSP that was manned at all times. The facility was monitored by closed circuit television via the URE security desk at all times.

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 "Lower" VRF and a "Severe" VSL.

SPP RE discovered that URE did not uniquely log visitors into its computer PCC that is within URE's PSP, if the visitor had signed in at the front entrance of the facility. The visitor log book at the PCC was used solely for visitors who had not logged in at the front entrance of the facility. The entrance into the PCC was considered an access point into URE's PSP rather than the front entrance. Therefore, URE should have had a method of logging all visitors that entered its PCC at the PSP access point as required by CIP-006-1 R4.

Therefore, SPP RE determined that URE was in violation of CIP-006-1 R4 because it could not provide evidence that proper logging and monitoring occurred when a visitor enters the PSP of the PCC.

In addition, SPP RE discovered that URE did not have a formal logging process as some facilities as required by CIP-006-3 R6. In one facility, doors were accessed using a key, therefore a manual log was required, and the evidence showed that not all URE personnel were properly logged into facility PSP.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the inability to uniquely log all visitor and URE personnel ingress and egress hinders URE's ability to protect its CCAs. Furthermore, without proper documentation, it would be impossible for physical security events to be sufficiently investigated and for the PSP to be adequately protected.

The risk to the reliability of the BPS was mitigated by the following factors. Visitors were required to be escorted by URE personnel while in the PSP. URE had implemented a process that includes visitors receiving visitor badges. The badges grant unescorted access to the PSP but record the visitor's use as the visitor enters and exits the badge reader-controlled PSP access control points. URE's badge reading logging system, which protects URE's PSPs other than the facility at issue, had no failures during the violation period.

CIP-007-1 R4

CIP-007-1 R4 provides:

> R4. Malicious Software Prevention — The Responsible Entity shall use anti-virus 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 anti-virus and malware prevention tools. In the case where anti-virus 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 anti-virus and malware prevention "signatures." The process must address testing and installing the signatures.

CIP-007-1 R4 has a "Medium" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that URE failed to request TFEs for Cyber Assets where it was not technically feasible to install anti-virus or anti-malware software, including communication switches and printers, in violation of R4.1.

Further, URE failed to test malware signature file updates prior to implementing the updates in the production environment anti-virus signatures had not been updated on one facility's workstations, in violation of R4.2.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE has anti-virus software installed on all of its workstations and servers to protect its network from malicious intrusion. URE had processes and procedures implemented for maintaining anti-virus and anti-malware software on the URE system to protect its Cyber Assets and CCAs. URE had anti-virus software and other malware prevention tools installed on its system where technically feasible. URE was conducting testing on its anti-virus servers prior to implementation on its production system. URE personnel were performing a daily check for host-based anti-virus signature updates and were evaluating any new signatures. URE personnel were checking for firewall-based anti-virus signatures or upgrades on a weekly basis and were utilizing the same signature testing process for host-based anti-virus signatures. URE conducts real-time monitoring of data packets that interact within the URE network. URE has not had any planned outages or systems failures on its system that protects its PSPs and ESPs.

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.

SPP RE determined that URE failed to 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, in violation of R5.

URE failed to provide evidence that user accounts throughout the company were implemented and approved by designated personnel, in violation of CIP-005-1 R5.1.1.

URE failed to require that all passwords used throughout the company consist of a combination of alpha, numeric, and "special" characters, in violation of CIP-007-1 R5.3.2. URE also failed to update its database passwords at least annually, in violation of CIP-007-1 R5.3.3.

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

URE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failures may have resulted in unauthorized access to URE's Cyber Assets and put the URE system at risk. Inadequate password requirements and failure to ensure password changes could increase the risk of unauthorized individuals with malicious intent gaining access to URE's Cyber Assets. The risk to the reliability of the BPS was mitigated by the following factors. Only employees with authorized physical access to the PCC and generation facilities which house URE's CCA information had access to these facilities. Further, URE did have an account management policy established, implemented, and documented for some of its groups. The policy adequately addressed the use of shared, generic, and administrator accounts, as well as removal of access to these accounts when necessary. URE reviewed the user accounts each time a patch was applied to the system. No system events occurred on the URE system during the violation period.

CIP-007-1 R7
CIP-007-1 R7 provides:

> 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.
>
> > R7.1. Prior to the disposal of such assets, the Responsible Entity shall destroy or erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
> >
> > R7.2. Prior to redeployment of such assets, the Responsible Entity shall, at a minimum, erase the data storage media to prevent unauthorized retrieval of sensitive cyber security or reliability data.
> >
> > R7.3. The Responsible Entity shall maintain records that such assets were disposed of or redeployed in accordance with documented procedures.

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

SPP RE determined that one group within URE failed to establish and implement formal methods, processes, and procedures for disposal or redeployment of Cyber Assets within the ESP, in violation of CIP-007-1 R7.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The risk was mitigated by several factors. Two URE groups follow a procedure, which addressed the requirements of CIP-007-1 R7. URE's group at issue has an arrangement with a vendor to come on-site and securely shred data storage media if needed.

CIP-007-1 R9

CIP-007-1 R9 provides:

R9. Documentation Review and Maintenance — The Responsible Entity shall review and update the documentation specified in Standard CIP-007 at least annually. Changes resulting from modifications to the systems or controls shall be documented within ninety calendar days of the change.

CIP-007-1 R9 has a "Lower" VRF and a "Severe" VSL.

SPP RE determined that URE failed to demonstrate that all required documentation reviews had been performed, in violation of CIP-007-1 R9. Two URE groups could not demonstrate that the following had been reviewed annually: 1) processes for ensuring ports and services were enabled and disabled; and 2) account management policies and controls, and security status monitoring.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's corporate processes and procedures showed revision dates for three consecutive years. Therefore, an information annual review occurred. URE had implemented procedures that afforded the protections of the CIP Reliability Standards for its PCC, such as an ESP with identified and monitored electronic access points, and a deny-by-default control model that protected associated ports and services. URE was manually reviewing its access logs at both the PCC and the BCC, and has implemented a process for reporting unusual activity on its system. No cyber security events have occurred on the URE system during the pendency of this violation.

CIP-008-1 R1

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

CIP-008-1 R1 provides in pertinent part:

> The Responsible Entity shall comply with the following requirements of Standard CIP-008:
>
> R1. Cyber Security Incident Response Plan — The Responsible Entity shall develop and maintain a Cyber Security Incident response plan. The Cyber Security Incident Response plan shall address, at a minimum, the following:
>
> > R1.1. Procedures to characterize and classify events as reportable Cyber Security Incidents.
> >
> > R1.2. Response actions, including roles and responsibilities of incident response teams, incident handling procedures, and communication plans.
> >
> > R1.3. Process for reporting Cyber Security Incidents to the Electricity Sector Information Sharing and Analysis Center (ES ISAC). The Responsible Entity must ensure that all reportable Cyber Security Incidents are reported to the ES ISAC either directly or through an intermediary.
> >
> > R1.4. Process for updating the Cyber Security Incident response plan within ninety calendar days of any changes.
> >
> > R1.5. Process for ensuring that the Cyber Security Incident response plan is reviewed at least annually.
> >
> > R1.6. Process for ensuring the Cyber Security Incident response plan is tested at least annually. A test of the incident response plan can range from a paper drill, to a full operational exercise, to the response to an actual incident.

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

SPP RE determined that one of URE's groups failed to have a cyber security incident response plan (Plan), in violation of CIP-008-1 R1. The group provided a Plan, but the Plan did not address requirements R1.1, R1.3, R1.4, and R1.5. Additionally, the group did not provide evidence that it had tested the 2011 Plan, in violation of R1.6.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The other URE groups had a Plan in place and had tested their Plan. The Plans tested by those two groups applied to the bulk of the Critical Assets and CCAs. URE had no reportable incidents during the violation period.

CIP-009-1 R1

CIP-009-1 R1 provides:

> The Responsible Entity shall comply with the following requirements of Standard CIP-009:
>
> > 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-09-1 R1 has a "Medium" VRF and a "Severe" VSL.

SPP RE determined that one of URE's groups failed to provide evidence of a documented recovery plan for CCAs, in violation of CIP-009-1 R1.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The group at issue had a disaster recovery plan that described actions for recovery of Cyber Assets, not CCAs. The disaster recovery plan provided some level of protection of the Cyber Assets and referenced another group's participation in the recovery process. The other URE groups had documented recovery plans for CCAs in place and had evidence of successful tests performed on the respective plans.

CIP-009-1 R4

CIP-009-1 R4 provides: "Backup and Restore — The recovery plan(s) shall include processes and procedures for the backup and storage of information required to successfully restore Critical Cyber Assets. For example, backups may include spare electronic components or equipment, written documentation of configuration settings, tape backup, etc."

CIP-009-1 R4 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that one of URE's groups failed to have documented processes and procedures for the backup and storage of information required to restore CCAs, in violation of CIP-009-1 R4.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Tape backups were performed, and the backup logs were manually reviewed by URE personnel. URE was testing the effectiveness of the backup process by randomly picking a restore of a server or workstation directory and verifying against copies of the original files.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of one hundred thousand dollars ($100,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. URE's violation was determined not to be an aggravating factor in the penalty determination;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violations, which was considered a neutral factor in the penalty determination because it was not applied throughout the company;
4. the small size of URE's operations, which was considered a mitigating factor in the penalty determination;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and

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

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of one hundred thousand dollars ($100,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[6]

CIP-002-1 R3
URE's Mitigation Plan to address its violation of CIP-002-1 R3 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006986 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to revise its CCA list to include the relays at the facility.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-003-1 R5
URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006987-2 and was submitted as non-public information to FERC in accordance with FERC orders.[7]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;

[6] *See* 18 C.F.R § 39.7(d)(7).
[7] URE submitted two previous versions of the Mitigation Plan to SPP RE. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

2. provide an attestation signed by senior management that Approach 1 had been adopted;
3. revise its Critical Asset Methodology used to identify URE Critical Assets;
4. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
5. document, based on the new Critical Asset list, an updated list of all Cyber Assets;
6. revise its CIP-003-3 R4 Information Protection Program and CIP-003-3 R5 Authorized Signatory document;
7. revise the NERC Access Request form to detail, in sufficient granularity, the specific access rights individuals are granted; and
8. review and revise the list of employees and contractors by name, title, and electronic systems and/or physical assets in which they have access. This review included confirmation that access privileges are correct and correspond with appropriate business requirements for personnel and/or contractors roles and responsibilities. URE will verify the list annually.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-004-1 R3

URE's Mitigation Plan to address its violation of CIP-004-1 R3 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007856-1 and was submitted as non-public information to FERC in accordance with FERC orders.[8]

URE's Mitigation Plan required URE to:

1. complete PRAs for individuals named in the Compliance Audit report and provide the date of the completed PRAs; and
2. have SPP RE review the completed PRAs on-site for verification.

[8] URE submitted a previous version of the Mitigation Plan. Version 1 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-004-1 R4

URE's Mitigation Plan to address its violation of CIP-004-1 R4 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007263-2 and was submitted as non-public information to FERC in accordance with FERC orders. [9]

URE's Mitigation Plan required URE to:

1. develop Cyber Security Program documentation that defines employee responsibilities for physical and/or electronic access to URE facilities, IT systems, and company documentation. The revised documentation describes departmental ownership for maintenance, quarterly review, and processes to follow for changes when employees' or contractors' status change;
2. document the process for controlling the addition, removal, monitoring, and overall management of specific physical and electronic access levels for all employees and/or contractors, including validation records. The process includes revocation within 24 hours for terminations due to cause, seven calendar days when access levels change, and quarterly review of electronic access lists; and
3. perform a review of personnel in accordance with its processes and procedures.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-005-1 R2

URE's Mitigation Plan to address its violation of CIP-005-1 R2 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is

[9] URE submitted two previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

designated as SPPMIT007206-3 and was submitted as non-public information to FERC in accordance with FERC orders.[10]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list;
4. revise URE's ESP diagrams;
5. remove the firewall rules that were at issue and provide evidence of removal;
6. address the interactive access authentication issue and provided evidence of the solution; and
7. document the technical solution.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-005-1 R1

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is

[10] URE submitted three previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in version 4 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE because URE did not include requesting TFEs if necessary in the plan. Version 3 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

designated as SPPMIT007204-2 and was submitted as non-public information to FERC in accordance with FERC orders.[11]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list;
4. revise each ESP diagram and all electronic access points to its ESP(s);
5. submit a TFE that was accepted by SPP RE covering assets that cannot support anti-virus/anti-malware;
6. document and submit password change logs to evidence passwords were changed in accordance with the standard on each EACM; and
7. change local, domain and database passwords and documented when the passwords were changed.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-005-1 R4 and CIP-007-1 R8

URE's Mitigation Plans to address its violation of CIP-005-1 R4 and CIP-007-1 R8 were submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this

[11] URE submitted two previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

violation is designated, respectively, as SPPMIT007183-2 and SPPMIT007182-2 and was submitted as non-public information to FERC in accordance with FERC orders.[12]

URE's Mitigation Plans required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list;
4. complete its most recent CVA and prepared Corrective Actions Plans (Action Plan) to address found vulnerabilities;
5. provide the status of the CVA Action Plan; and
6. documented the use of cyber security software to address password complexity per CIP-007-3 R5.3.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-006-1 R6

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

[12] URE submitted two previous versions of both Mitigation Plans. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

designated as SPPMIT007857-2 and was submitted as non-public information to FERC in accordance with FERC orders.[13]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list;
4. revise its PSP diagrams to identify entry points, access controls and the complete boundary of the PSP more clearly; and
5. test controls at each of the entry points to the PSPs and documented the results of the testing.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R2

URE's Mitigation Plan to address its violation of CIP-007-1 R2 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007172-3 and was submitted as non-public information to FERC in accordance with FERC orders.[14]

[13] URE submitted two previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

[14] URE submitted three previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 4 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE because URE did not include requesting TFEs if necessary in the plan. Version 3 was rejected by SPP RE

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list; and
4. revise its baseline ports and services documentation.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R3

URE's Mitigation Plan to address its violation of CIP-007-1 R3 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007173-3 and was submitted as non-public information to FERC in accordance with FERC orders.[15]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;

to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

[15] URE submitted three previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 4 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE because URE did not include requesting TFEs if necessary in the plan. Version 3 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

a. provide an attestation signed by senior management that Approach 1 had been adopted; and

b. revise its Critical Asset Methodology used to identify URE Critical Assets;

2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list;
4. document its patch update availability sources;
5. perform and submit samples of the 30-day patch assessment; and
6. submit evidence that the patch relevant to the violation is no longer pending on the applicable Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R6

URE's Mitigation Plan to address its violation of CIP-007-1 R6 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007181-3 and was submitted as non-public information to FERC in accordance with FERC orders.[16]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;

    a. provide an attestation signed by senior management that Approach 1 had been adopted; and

[16] URE submitted three previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 4 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE because URE did not include requesting TFEs if necessary in the plan. Version 3 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

b. revise its Critical Asset Methodology used to identify URE Critical Assets;

2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management;
3. document an updated list of all Cyber Assets based on the new Critical Asset list; and
4. perform reviews of the SCADA/EMS application data logs and provide evidence of the daily log checks.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-009-1 R2

URE's Mitigation Plan to address its violation of CIP-009-1 R2 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007185-2 and was submitted as non-public information to FERC in accordance with FERC orders.[17]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management; and
3. document an updated list of all Cyber Assets based on the new Critical Asset list.

[17] URE submitted two previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R1

URE's Mitigation Plan to address its violation of CIP-007-1 R1 was submitted to SPP RE . The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007171-2 and was submitted as non-public information to FERC in accordance with FERC orders.[18]

URE's Mitigation Plan required URE to:

1. adopt Approach 1 to utilize the CIP Version 4 Bright-Line Criteria to identify Critical Assets consistent with the September 5, 2013, NERC Revised Transition Guidance;
    a. provide an attestation signed by senior management that Approach 1 had been adopted; and
    b. revise its Critical Asset Methodology used to identify URE Critical Assets;
2. revise its Critical Asset List to reflect that the facility had been removed from the list based on the adoption of Approach 1. The Critical Asset List was approved and signed by senior management; and
3. document an updated list of all Cyber Assets based on the new Critical Asset list.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-003-1 R6

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is

[18] URE submitted two previous versions of the Mitigation Plan. Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in Version 3 of the Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

designated as SPPMIT007179-1 and was submitted as non-public information to FERC in accordance with FERC orders.[19]

URE Mitigation Plan required URE to:

1. revise its CCCM plan to ensure that each in-scope department is included in the plan;
2. ensure that that the CCCM approval forms are incorporated in the plan;
3. identify any software required for implementation; and
4. test the change control process for readiness.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-005-1 R5

URE's Mitigation Plan to address its violation of CIP-005-1 R5 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007180-2 and was submitted as non-public information to FERC in accordance with FERC orders.[20]

URE's Mitigation Plan required URE to:

1. submit weekly activity attendance and sign off sheets to evidence the documentation and maintenance requirements in CIP-005-3 R5;
2. document and submit baseline ports and services; and
3. submitted firewall rule sets to document the ports and services allowed.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

[19] Version 1 of this Mitigation Plan was rejected by the SPP RE by request of both the SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in the amended Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner.

[20] Version 1 was rejected by the SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

CIP-006-1 R1

URE's Mitigation Plan to address its violation of CIP-006-1 R1 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007310-2 and was submitted as non-public information to FERC in accordance with FERC orders.[21]

URE's Mitigation Plan required URE to:

1. adopt CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset methodology used to identify URE Critical Assets;
3. revise its Critical Asset list to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document an updated list of all Cyber Assets based on the new Critical Asset list;
5. revise its PCC and BCC PSP documentation to identify entry access points, access controls and the complete boundary of the PSP more clearly;
6. implement card readers at each URE PSP access point, integrate the newly implemented card readers into the system;
7. test and confirm card reader integration to ensure proper functioning; and
8. revise URE's PSP to document alternative controls for physical access in the event of a failure.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-006-1 R1.8

URE's Mitigation Plan to address its violation of CIP-006-1 R1.8 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007314-2 and was submitted as non-public information to FERC in accordance with FERC orders.[22]

[21] Version 1 of this Mitigation Plan was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.
[22] Version 1 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

URE's Mitigation Plan required URE to:

1. adopt the CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update a list of all Cyber Assets based on the new Critical Asset list;
5. document testing of the URE PAC systems per CIP-007-3 R1;
6. revise its security patch update documentation per CIP-007-3 R3 for its PAC systems;
7. revise its anti-virus and anti-malware procedure per CIP-007-3 R4 for its PAC systems;
8. test and implement the signature files;
9. complete its 2013 CVA and prepare corrective actions plan to address found vulnerabilities; and
10. provide the status of the CVA action plan.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-006-1 R2

URE's Mitigation Plan to address its violation of CIP-006-1 R2 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007311-2 and was submitted as non-public information to FERC in accordance with FERC orders.[23]

URE's Mitigation Plan required URE to:

1. adopt CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list . The Critical Asset List was approved and signed by senior management; and
4. document and update its list of all Cyber Assets based on the new Critical Asset list.

[23] Version 1 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-006-1 R3

URE's Mitigation Plan to address its violation of CIP-006-1 R3 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007312-2 and was submitted as non-public information to FERC in accordance with FERC orders.[24]

URE's Mitigation Plan required URE to:

1. adopt CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update list of all Cyber Assets based on the new Critical Asset list;
5. revise all PSP diagrams to more clearly identify entry points, access controls and the complete boundary of the PSP; and
6. test controls at each of the entry points into the PSP.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-006-1 R4

URE's Mitigation Plan to address its violation of CIP-006-1 R4 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007313-1 and was submitted as non-public information to FERC in accordance with FERC orders.[25]

[24] Version 1 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

[25] Version 1 of this Mitigation Plan was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in the amended Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner.

URE's Mitigation Plan required URE to:

1. revise the visitor access policy to ensure that each visitor is uniquely identified by badge and that the time of access at each PSP access point is properly logged and monitored by URE security staff at all times;
2. create visitor badges that uniquely log a visitors' access into and out of the PSPs;
3. implement processes to ensure that each access point into its PSPs has card reader access control with monitoring and logging incorporated into the system; and
4. raise the BCC walls up to the roof to eliminate the gap above the false ceiling.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R4

URE's Mitigation Plan to address its violation of CIP-007-1 R4 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007174-2 and was submitted as non-public information to FERC in accordance with FERC orders.[26]

URE's Mitigation Plan required URE to:

1. adopt CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update its list of all Cyber Assets based on the new Critical Asset list;
5. revise its anti-virus and anti-malware procedures, implemented and tested the corresponding signature files; and
6. submit a TFE covering assets that cannot support anti-virus and anti-malware. The TFE has been accepted by SPP RE.

[26] Version 1 of this Mitigation Plan was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R5

URE's Mitigation Plan to address its violation of CIP-007-1 R5 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007175-2 and was submitted as non-public information to FERC in accordance with FERC orders.[27]

URE's Mitigation Plan required URE to:

1. adopt CIP Version 4 bright-line criteria to identify Critical Assets e;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update its list of all Cyber Assets based on the new Critical Asset list;
5. address password complexity per CIP-007-3 R5.3; and
6. submit TFEs covering some the assets at issue. The TFEs have been accepted.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R7

URE's Mitigation Plan to address its violation of CIP-007-1 R7 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007176-2 and was submitted as non-public information to FERC in accordance with FERC orders.[28]

URE's Mitigation Plan required URE to:

1. adopt the CIP Version 4 bright-line criteria to identify Critical Assets;

[27] Version 1 of this Mitigation Plan was rejected by SPP RE.
[28] Version 1 of this Mitigation Plan was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update its list of all Cyber Assets based on the new Critical Asset list; and
5. revise its disposal and redeployment process documentation to clarify what actions should be taken by URE personnel when assets need to be removed from URE's ESPs and PSPs for disposal or redeployment.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-007-1 R9

URE's Mitigation Plan to address its violation of CIP-007-1 R9 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007184-3 and was submitted as non-public information to FERC in accordance with FERC orders.[29]

URE's Mitigation Plan required URE to:

1. adopt the CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management;
4. document and update its list of all Cyber Assets based on the new Critical Asset list;
5. revise its CIP-007-3 R1 test procedure documentation to ensure that ports and services are enabled/disabled per CIP-007-1 R2;
6. ensure that its account management policies and controls reflect the requirements of CIP-007-1 R5;

[29] Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in the amended Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

7. ensure that the security status monitoring required by CIP-007-1 R6 is completed annually; and
8. perform and document an annual review.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-008-1 R1

URE's Mitigation Plan to address its violation of CIP-008-1 R1 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007177-2 and was submitted as non-public information to FERC in accordance with FERC orders.[30]

URE's Mitigation Plan required URE to:

1. revise the URE Cyber Security Incident Response Plan.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-009-1 R1

URE's Mitigation Plan to address its violation of CIP-009-1 R1 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007178-1 and was submitted as non-public information to FERC in accordance with FERC orders.[31]

URE's Mitigation Plan required URE to:

1. create an Annual Recovery Exercise Team that is tasked with the annual review of Recovery Plan for CCAs in the URE system; and

[30] Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in the amended Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner. Version 2 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.

[31] Version 1 was rejected by SPP RE by request of both SPP RE and URE because URE wanted to perform an internal review of its entire CIP program. Also, in the amended Mitigation Plan, URE set realistic goals that evidence would be provided to SPP RE in a timely manner.

2. document and review its 2012 CCA Recovery Plans.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-009-1 R4

URE's Mitigation Plan to address its violation of CIP-009-1 R4 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007186-2 and was submitted as non-public information to FERC in accordance with FERC orders.[32]

URE's Mitigation Plan required URE to:

1. adopt the CIP Version 4 bright-line criteria to identify Critical Assets;
2. revise its Critical Asset Methodology used to identify URE Critical Assets;
3. revise its Critical Asset List to reflect that the facility had been removed from the list. The Critical Asset List was approved and signed by senior management; and
4. document and update its list of all Cyber Assets based on the new Critical Asset list.

URE certified that the above Mitigation Plan requirements were completed and submitted evidence of completion of its Mitigation Plan to SPP RE. After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[33]

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,[34] the

[32] Version 1 was rejected by SPP RE to allow URE to revise the Mitigation Plan to reflect the correct mitigation activities based on third-party consultation and outreach.
[33] *See* 18 C.F.R. § 39.7(d)(4).
[34] *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

NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2013. The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of a one hundred thousand dollar ($100,000) 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's violation history was determined not to be an aggravating factor in the penalty determination;
2. URE was cooperative throughout the compliance enforcement process;
3. URE had a compliance program at the time of the violations, which was considered a neutral factor in the penalty determination because it was not applied throughout the company;
4. the small size of URE's operations, which was considered a mitigating factor in the penalty determination;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. the violations did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred thousand dollars ($100,000) 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.

¶ 61,069 (2009); *North American Electric Reliability Corporation*, "Notice of No Further Review and Guidance Order," 132 FERC ¶ 61,182 (2010).

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 SPP RE and URE, included as Attachment a;

b) SPP RE's Source document, included as Attachment b;

c) Record documents for the violation of CIP-002-1 R3; R3.2, included as Attachment c:

   1. URE's Mitigation Plan designated as SPPMIT006986;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

d) Record documents for the violation CIP-003-1 R5; R5.1, included as Attachment d:

   1. URE's Mitigation Plan designated as SPPMIT006987-2
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

e) Record documents for the violation CIP-004-1 R3; R3.1, included as Attachment e:

   1. URE's Mitigation Plan designated as SPPMIT007856-1 submitted November 7, 2013;

2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

f) Record documents for the violation CIP-004-1 R4, included as Attachment f:
   1. URE's Mitigation Plan designated as SPPMIT007263-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

g) Record documents for the violation CIP-005-1 R2; R2.1; R2.2; R2.4, included as Attachment g:
   1. URE's Mitigation Plan designated as SPPMIT007206-3 submitted November 8, 2013;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

h) Record documents for the violation CIP-005-1 R1, included as Attachment h:
   1. URE's Mitigation Plan designated as SPPMIT007204-2 submitted November 13, 2013;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

i) Record documents for the violation CIP-005-1 R4; R4.1; R4.2; R4.3; R4.4; R4.5, included as Attachment i:
   1. URE's Mitigation Plan designated as SPPMIT007183-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

j) Record documents for the violation CIP-007-1 R8; R8.1; R8.2; R8.4, included as Attachment j:
   1. URE's Mitigation Plan designated as SPPMIT007182-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

k) Record documents for the violation CIP-006-1 R6, included as Attachment k:
   1. URE's Mitigation Plan designated as SPPMIT007857-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

l) Record documents for the violation CIP-007-1 R2; R2.1; R2.2, included as Attachment l:
   1. URE's Mitigation Plan designated as SPPMIT007172-3;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

m) Record documents for the violation CIP-007-1 R3, included as Attachment m:
   1. URE's Mitigation Plan designated as SPPMIT007173-3;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

n) Record documents for the violation CIP-007-1 R6; R6.5, included as Attachment n:
   1. URE's Mitigation Plan designated as SPPMIT007181-3;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

o) Record documents for the violation CIP-009-1 R2, included as Attachment o:
   1. URE's Mitigation Plan designated as SPPMIT007185-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

p) Record documents for the violation CIP-007-1 R1; R1.1, included as Attachment p:
   1. URE's Mitigation Plan designated as SPPMIT007171-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

q) Record documents for the violation CIP-003-1 R6, included as Attachment q:
   1. URE's Mitigation Plan designated as SPPMIT007179-1;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

r) Record documents for the violation CIP-005-1 R5.1; R5.3, included as Attachment r:
   1. URE's Mitigation Plan designated as SPPMIT007180-2;

2. URE's Certification of Mitigation Plan Completion dated;
3. SPP RE's Verification of Mitigation Plan Completion dated;

s) Record documents for the violation CIP-006-1 R1.1; R1.2; R1.4; R1.6 , included as Attachment s:
   1. URE's Mitigation Plan designated as SPPMIT007310-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

t) Record documents for the violation CIP-006-2 R2.2, included as Attachment t:
   1. URE's Mitigation Plan designated as SPPMIT007314-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

u) Record documents for the violation CIP-006-1 R2, included as Attachment u:
   1. URE's Mitigation Plan designated as SPPMIT007311-2;
   2. URE's Certification of Mitigation Plan Completion dated November 7, 2013;
   3. SPP RE's Verification of Mitigation Plan Completion dated November 12, 2013;

v) Record documents for the violation CIP-006-1 R3, included as Attachment v:
   1. URE's Mitigation Plan designated as SPPMIT007312-2 submitted November 8, 2013;
   2. URE's Certification of Mitigation Plan Completion dated November 8, 2013;
   3. SPP RE's Verification of Mitigation Plan Completion dated November 12, 2013;

w) Record documents for the violation CIP-006-1 R4, included as Attachment w:
   1. URE's Mitigation Plan designated as SPPMIT007313-1;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

x) Record documents for the violation CIP-007-1 R4, included as Attachment x:
   1. URE's Mitigation Plan designated as SPPMIT007174-2;
   2. URE's Certification of Mitigation Plan Completion;
   3. SPP RE's Verification of Mitigation Plan Completion;

y) Record documents for the violation CIP-007-1 R5, included as Attachment y:

1. URE's Mitigation Plan designated as SPPMIT007175-2;
2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

z) Record documents for the violation CIP-007-1 R7, included as Attachment z:

1. URE's Mitigation Plan designated as SPPMIT007176-2;
2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

aa) Record documents for the violation CIP-007-1 R9, included as Attachment aa:

1. URE's Mitigation Plan designated as SPPMIT007184-3;
2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

bb) Record documents for the violation CIP-008-1 R1.1; R1.3; R1.4; R1.5; R1.6, included as Attachment bb:

1. URE's Mitigation Plan designated as SPPMIT007177-2;
2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

cc) Record documents for the violation CIP-009-1 R1, included as Attachment cc:

1. URE's Mitigation Plan designated as SPPMIT007178-1;
2. URE's Certification of Mitigation Plan Completion;
3. SPP RE's Verification of Mitigation Plan Completion;

dd) Record documents for the violation CIP-009-1 R4, included as Attachment dd:

1. URE's Mitigation Plan designated as SPPMIT007186-2;
2. URE's Certification of Mitigation Plan Completion; and
3. SPP RE's Verification of Mitigation Plan Completion.

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Tasha Ward* Compliance Enforcement Attorney Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223-4936 (501) 688-1738 (501) 482-2025-facsimile tward.re@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223-4936 (501) 688-1672 (501) 482-2025 – facsimile jgertsch.re@spp.org	Sonia C. Mendonça* Assistant General Counsel and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* North American Electric Reliability Corporation Senior Counsel and Associate Director, Enforcement Processing 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net Ron Ciesiel* General Manager Southwest Power Pool Regional Entity 200 Worthen Drive Little Rock, AR 72223-4936 (501) 614-3265 (501) 482-2025 – facsimile rciesiel.re@spp.org *Persons to be included on the Commission's service list are indicated with an asterisk. NERC requests waiver of the Commission's rules and regulations to permit the inclusion of more than two people on the service list.

Conclusion

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

Respectfully submitted,

/s/ Sonia Mendonça

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

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

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

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

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments