PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

December 31, 2012

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

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

Dear Ms. Bose:

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

This Notice of Penalty is being filed with the Commission because the 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-003-1 R5.2, CIP-003-1 R6, CIP-007-1 R4.2, CIP-007-1 R9, CIP-004-3 R4.1 and R4.2, CIP-005-1 R1, CIP-002-1 R2, CIP-005-1 R4.2, CIP-006-1 R1.1 and R1.8, CIP-007-1 R3.2, CIP-007-1 R5.2, R5.2.3 and R5.3.3, CIP-005-1 R2.2 and R2.6, CIP-004-3 R2.1, CIP-004-3 R3, CIP-004-3 R4.1 and R4.2, and CIP-007-3 R4.1 and R4.2. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred fifty-three thousand dollars ($153,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement.

---

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

[2] *See* 18 C.F.R § 39.7(c)(2).

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

Accordingly, the violations identified as NERC Violation Tracking Identification Numbers: SPP201000425, SPP201000426, SPP201000428, SPP201100528, SPP201100568, SPP201100569, SPP201100604, SPP201100605, SPP201100607, SPP201100608, SPP201100609, SPP201100610, SPP2012009547, SPP2012009760, SPP2012009983, and SSP2012009592 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 27, 2012, 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 (2012), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

Region	Registered Entity	NOC ID	NERC Violation ID	Reliability Std.	Req. (R)	VRF	Total Penalty
Southwest Power Pool Regional Entity	Unidentified Registered Entity	NOC-1717	SPP201000425	CIP-003-1	R5.2	Lower	$153,000
			SPP201000426	CIP-003-1	R6	Lower	
			SPP201000428	CIP-007-1	R4.2	Lower	
			SPP201100528	CIP-007-1	R9	Lower	
			SPP201100568	CIP-004-3	R4.1, R4.2	Lower	
			SPP201100569	CIP-005-1	R1	Medium	
			SPP201100604	CIP-002-1	R2	Lower	

			SPP201100605	CIP-005-1	R4.2	Medium	
			SPP201100607	CIP-006-1	R1.1, R1.8	Medium Lower	
			SPP201100608	CIP-007-1	R3.2	Lower	
			SPP201100609	CIP-007-1	R5.2, R5.2.3, R5.3.3	Lower Medium Medium	
			SPP201100610	CIP-005-1	R2.2, R2.6	Medium Lower	
			SPP2012009547	CIP-004-3	R2.1	Medium	
			SPP2012009983[4]	CIP-004-3	R3	Medium	
			SPP2012009760[5]	CIP-004-3	R4.1, R4.2	Lower	
			SPP2012009592	CIP-007-3	R4.1, R4.2	Medium	

CIP-003-1 R5.2 (SPP201000425)

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[6] shall document and implement a program for managing access to protected Critical Cyber Asset information.

[4] The Settlement Agreement states the SPP2012009983 violation is CIP-004-3 R4 (R4.1 and R4.2).
[5] The Settlement Agreement states the SPP2012009760 violation is CIP-004-3 R3.
[6] Within the text of the CIP Standards referenced in this Full Notice of Penalty, "Responsible Entity" shall mean Reliability Coordinator, Balancing Authority, Interchange Authority, Transmission Service Provider, Transmission Owner, Transmission Operator, Generator Owner, Generator Operator, Load Serving Entity, NERC, and Regional Reliability Organizations.

> R5.2 The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the Responsible Entity's needs and appropriate personnel roles and responsibilities.

CIP-003-1 R5.2 has a "Lower" Violation Risk Factor (VRF) and a "Severe" Violation Severity Level (VSL).

URE self-reported a violation of CIP-003-1 R5.2 because it did not have documentation to demonstrate that it had performed an annual review of personnel with access rights to two areas containing Critical Cyber Asset (CCA) information. The areas at issue included a SharePoint site related to URE's network services and an Energy Management System (EMS) information folder on a network drive.

SPP RE determined that URE violated CIP-003-1 R5.2 for its failure to review at least annually the access privileges to protected information to confirm that access privileges are correct and that they correspond with the URE's needs and appropriate personnel roles and responsibilities.

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

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the bulk power system (BPS). The physical, domain, and remote access rights of personnel having access to the network services and EMS information had been removed at the time of the termination of their employment, despite the lack of annual review. These actions prevented access to the CCAs at issue despite URE's failure to review the applicable access list annually.

<u>CIP-003-1 R6 (SPP201000426)</u>
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 "Lower" VSL.

URE self-reported a violation of CIP-003-1 R6 related to the execution of its change control and configuration management process for CCAs. Although a change management process had been established, URE indicated that some of the change management documents lacked: 1) supervisory approval; 2) supervisory and managerial approval; 3) a change implementation date; 4) a notification date to affected groups by change; and 5) an implementation date.

SPP RE determined that URE violated CIP-003-1 R6 for its failure to document its change control and configuration management process.

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

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by several factors. First, although URE lacked some documentation to evidence its change control and configuration management process, the process was fully implemented, URE had a multi-tiered approach to change management that minimized the risk of system changes being made without some preliminary level of review and approval. For example, prior to initiating the change control process for a hardware and software component, a change control request must be submitted to department supervisors or project sponsors, if the change is requested by the business division. The change control request then must be submitted to a board for review and scrutiny. The board is responsible for governance of URE's Information Technology division. Second, board approvals were received in each instance for which a change had been requested during the violation period, thereby reducing the risk to the BPS.

CIP-007-1 R4.2 (SPP201000428)

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 R4.2 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).

> R4.2 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 R4.2 has a "Lower" VRF and a "High" VSL.

URE self-reported a violation of CIP-007-1 R4.2 related to the implementation and maintenance of anti-virus prevention signatures displayed as data files. Computer to computer communication issues, involving servers established to administer virus updates, prevented automated virus-identifying data file updates on the URE energy management system (EMS) servers. URE was under the incorrect impression that the EMS servers were utilizing the appropriate protocols to allow communication to the anti-virus servers. URE later determined that the EMS servers' communication to the anti-virus servers was blocked. Although anti-virus software was installed, regular updates to the software were not occurring.

SPP RE determined that URE violated CIP-007-1 R4.2 for its failure to implement a process for the update of anti-virus and malware prevention "signatures."

SPP RE determined the duration of the violation to be from J the date the Standard became mandatory and enforceable to URE to the date the servers were updated with the required data files.

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 risk was mitigated by several factors. First, the EMS servers at issue resided behind the URE electronic security perimeter (ESP) firewall, which reduced malware exposure by restricting Internet access via firewall rule sets. Second, anti-virus software was active on the servers despite the lack of automated updating.

<u>CIP-007-1 R9 (SPP201100528)</u>
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 "High" VSL.

URE self-reported a violation of CIP-007-3 R9 related to its annual review of a process document for access management and an annual review of a process document for malicious software prevention. URE completed a review of its access management document. A draft of a modified document for access management was submitted for review and approval. Although the document was reviewed and there were no substantive changes to the overall functional process, the modified document for access management did not receive a final approval the following year. No review of the process document for malicious software prevention could be identified.

SPP RE determined that URE violated CIP-007-3 R9 for its failure to review and update the documentation specified in Standard CIP-007-1 at least annually.

SPP RE determined the duration of the violation to be from the date by which the annual reviews were required to receive final review through the date by which both documents had been reviewed and formally approved.

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Although URE did not submit its CIP-007-1 documents for a final review, no substantive changes were made to the documents during the review phase. Additionally, the prior year's approved versions of both the malicious software prevention document and access management document were still in active use with no loss of capability to appropriately manage access to Cyber Assets. Anti-virus and malware prevention has continued uninterrupted to effectively provide protection to Cyber Assets, resulting in no compromise of Cyber Assets during the violation period.

CIP-004-3 R4.1 and R4.2 (SPP201100568)

The purpose statement of Reliability Standard CIP-004-3 provides: "Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered CIP-002-3 through CIP-009-3."

CIP-004-3 R4 provides:

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

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

CIP-004-3 R4.1 and R4.2 have a "Lower" VRF and a "Moderate" VSL.

URE self-reported a violation of CIP-004-3 R4.1. URE stated that no documentation could be produced to demonstrate that the list of personnel with access to CCAs had been reviewed quarterly. The quarterly review failures began and the required quarterly review process was not initiated until almost two years later. A total of eight quarterly reviews were not conducted.

URE self-reported a violation of CIP-004-3 R4.2 because URE failed to remove within the required seven-day timeframe the access of one EMS engineer when he was transferred to a working group where CCA access was no longer required. The individual was a system engineer in the EMS group responsible for normal support of the operating centers and building the database for an EMS conversion project. The individual's role required physical and electronic access to URE's EMS. In accordance with URE's corporate policy, the access revocation should have occurred, but access was not revoked until almost three months later.

SPP RE determined that URE violated CIP-004-3 R4.1 and R4.2 for its failure to review and update its list of personnel with access to CCAs quarterly, and for its failure to revoke personnel access to CCAs within seven calendar days.

SPP RE determined the duration of the first instance of noncompliance to be from the date the first quarterly review failure occurred to the date the required quarterly reviews were implemented. The duration of the second instance of noncompliance was from the day following the deadline for access revocation to the date the required access revocation occurred.

SPP RE determined that this violation posed a minimal risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the risk was mitigated by several factors. First, regarding the first instance of noncompliance, the terminated employees were present on the access list that URE failed to review on quarterly basis. URE verified that all employees at issue had had their physical, domain, and remote access removed at the time of their termination. Therefore, despite the failure to perform the required reviews, URE's cyber systems were protected against unauthorized access.

Second, regarding the second instance of noncompliance, the employee with the late access revocation was transferred to another working group and no longer required access to the CCAs. The individual remained an employee of URE, and URE did not identify any unauthorized access by the employee following the date when access revocation should have occurred.

CIP-005-1 R1 (SPP201100569)

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 CIP-002 through CIP-009."

CIP-005-1 R1 provides in pertinent part: "R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s)."

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

URE self-reported a violation of CIP-005-3a R1. URE had identified equipment as an electronic access point that did not meet the criteria associated with an access point to an ESP. Following further investigation by the SPP RE Audit Team during URE's Compliance Audit, it was determined that URE had identified its EMS front-end device as an ESP access point and a CCA. The front-end device should instead have been identified solely as a CCA.

In addition, URE failed to identify one ESP access point that supported remote terminal unit (RTU) traffic. URE properly identified the firewalls controlling routable protocol access into the ESP as access points but it failed to identify the access points where serial protocol traffic from the field RTUs entered the ESP. The RTU serial protocol traffic flows from the RTUs through the URE control center modems and then passes through a signal-switching device. The signal switching device (modem

sharing device) relays the information to the production EMS communication front-end devices and replicates that data to the quality assurance (Q/A) EMS communication front-end devices. Data from the production EMS flows back out to the RTUs via the signal-splitting device from a serial port expansion device on the production EMS front-end. However, data from the Q/A EMS is blocked to prevent improper operation of infrastructure assets.

URE later determined that the signal-switching device should have been logically identified as the ESP access point for both the RTU traffic and the EMS front-end.

SPP RE determined that URE violated CIP-005-1 R1 for its failure to identify and document all access points to the ESPs.

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

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The first instance of noncompliance involved a failure to identify the proper access point, and despite this identification failure, the device at issue was implementing and performing access control functions. The second instance of noncompliance was related to the RTU traffic. The RTU traffic crossing the device was non-routable and used leased line analog communication circuits. The implementation of such non-routable communications shields the devices from vulnerabilities that could be presented via a routable communication circuit, thereby reducing the risk to the BPS.

CIP-002-1 R2 (SPP201000604)

The purpose statement of Reliability Standard CIP-002-1 provides in pertinent part: "Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment."

CIP-002-1 R2 provides:

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

CIP-002-1 R2 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE determined that URE failed to identify a substation as a Critical Asset. The substation is in the electrical path of transmission lines used for initial system restoration as provided in the System Restoration Plan. CIP-002-1 R1 (R1.2.4) requires that an entity's risk-based assessment methodology (RBAM) consider systems and facilities critical to system restoration when conducting its Critical Asset determination. Further, in accordance with the RBAM and all revisions, URE was required by its Critical Asset Identification Worksheet to consider whether an asset is critical to system restoration when making its Critical Asset determinations.

In accordance with its criteria, URE accurately designated two of the blackstart combustion turbines as Critical Assets because of their role in system restoration. However, URE failed to designate the associated substation as a Critical Asset, despite the fact that it serves as the initial transmission interconnection for supplying the blackstart power for system restoration.

SPP RE determined that URE violated CIP-002-1 R2 for its failure to properly identify one Critical Asset and failed to include it in its list of Critical Assets.

SPP RE determined the duration of the violation to be from the date the Substation should have been designated as a Critical Asset to the date URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. Although the substation was not properly designated as a Critical Asset, the substation contained no CCAs. Therefore, there were no CCAs residing within the station that required compliance with the CIP Standards. Second, URE has redundancies built into the blackstart portion of its system restoration plan. The restoration plan designates both primary and alternate system restoration paths. Consequently, despite a potential loss of the substation, URE would have been able to use an alternate power station for blackstart initiation, thereby reducing the risk to the surrounding BPS associated with the loss of the station.

CIP-005-1 R4.2 (SPP201100605)

CIP-005-1 R4 provides in pertinent part:

> R4. Cyber Vulnerability Assessment — The Responsible Entity shall perform a cyber vulnerability assessment of the electronic access points to the Electronic Security

Perimeter(s) at least annually. The vulnerability assessment shall include, at a minimum, the following:

R4.2. A review to verify that only ports and services required for operations at these access points are enabled;

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

During the Compliance Audit, SPP RE determined that URE could not provide evidence that its enabled ports and services, as defined in its firewall rule sets, were being reviewed as part of URE's annual vulnerability assessment of its ESP's access points. URE relies on a vulnerability tool for performing automated vulnerability assessments. The tool identified the ports and services that the firewall device was responding to (*i.e.*, ports utilized to communicate with the firewall interface). However, the tool did not identify the ports configured in the firewall rule sets (*i.e.*, the ports and services that allow traffic to flow through the firewall). As a result, ports and services that were no longer required for operations may have remained enabled following the vulnerability assessment.

SPP RE determined that URE violated CIP-005-1 R4.2 for its failure to verify that only ports and services required for operations at the electronic access points to the ESPs were enabled.

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

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS. The risk was mitigated by several factors. First, the ports and services allowing access to the firewall interface were properly evaluated, thereby protecting the firewall from access via unauthorized ports. Second, the host machines being accessed through the firewall had only necessary ports enabled, and therefore, any unauthorized port traffic through the firewall would be blocked at the host machines, thereby minimizing the risk posed by malicious traffic crossing any not required ports. Third, the enabled ports and services were documented despite the lack of an annual review being conducted. Following a review of the 47 originally enabled firewall rules, it was determined that seven rules had not been utilized within 90 days and were therefore disabled.

CIP-006-1 R1.1 and R1.8 (SPP201100607)

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

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

CIP-006-1 R1 provides in pertinent part:

> R1. Physical Security Plan — The Responsible Entity shall create and maintain a physical security plan, approved by a senior manager or delegate(s) that shall address, at a minimum, the following:
>
> > R1.1. 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.
> >
> > ****
> >
> > R1.8. 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 R1.1 has a "Medium" VRF and R1.8 has a "Lower" VRF. Both Requirements have a "Severe" VSL.

In a Self-Report, URE reported a violation of CIP-006-3c R1.1 for its failure to establish a completely enclosed, "six-wall" boundary for two Physical Security Perimeters (PSPs). URE had incorrectly relied on a raised floor and dropped ceiling to establish its "six-wall" boundary.

Moreover, the SPP RE Audit Team discovered an additional instance of noncompliance during URE's Compliance Audit because one router supporting URE's EMS and located within an ESP, did not reside in a designated PSP.

In a second Self-Report, URE identified an additional instance of noncompliance with CIP-006-3c R2. Prior to a certain date, URE's recovery plan for Cyber Assets used in the access control and monitoring of its PSPs did not meet the content requirements of this Standard. Specifically, its recovery plans for

Critical Assets did not include recovery plans for access control and monitoring of physical control systems, as required by CIP-009-3 R1 and made applicable by CIP-006-3 R2.2.

Furthermore, during the Compliance Audit, the SPP RE Audit Team identified a violation of CIP-006-1 R1.1 because the network data cables between two of URE's PSPs were not enclosed within a six-wall boundary, nor had URE implemented alternative security measures or requested a Technical Feasibility Exception (TFE).

The SPP RE Audit Team also determined that URE had failed to review the server logs for its Physical Access Control Systems database, as required by CIP-007-3 R6.5.

Finally, regarding CIP-006-3 R2.2, the SPP RE Audit Team determined that not all Cyber Assets used for physical access control and monitoring were identified in URE's master CIP device list. URE had identified its servers but the workstations used for physical security monitoring in URE's security operations center were not identified. As a result, URE could not demonstrate that the non-listed assets were afforded the protective measures specified in CIP-006-3 R2.2.

SPP RE determined that URE violated CIP-006-1 R1.1 and R1.8 for failing to: 1) establish a completely enclosed, "six-wall" boundary for two PSPs and one router; 2) ensure that its recovery plan for Cyber Assets used in the access control and monitoring of its PSPs met the content requirements of this Standard; and 3) review the Microsoft SQL server logs for its database.

SPP RE determined the duration of the CIP-006-1 R1 router related instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date URE declared the newly defined PSP in which the router resides as an official NERC PSP.

SPP RE determined the duration of the CIP-006-1 R1 data cabling related instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date URE declared the newly defined PSP in which the data cabling resides as an official NERC PSP.

SPP RE determined the duration of the CIP-006-1 R11.8 recovery plan related instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date URE had officially approved a physical security system recovery plan.

SPP RE determined the duration of the CIP-006-1 R1.8 server log review related instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date URE implemented its procedure for log review.

SPP RE determined the duration of the CIP-006-1 R1.8 physical security server (master CIP device list) related instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date URE added the devices to the master CIP device list and ensured they were subject to the CIP requirements.

SPP RE determined the duration of the CIP-006-1 R1 six-wall boundary related instance of noncompliance to be from the date the Standard became mandatory and enforceable, through the date URE completed construction activities to ensure an appropriate six-wall boundary was in place.

SPP RE determined that this violation posed a minimal risk and not pose a serious or substantial risk to the reliability of the BPS. Although URE failed to completely enclose the PSP at its primary control center, the control center was continuously manned and located in a controlled access facility with security guards on duty. As a result, any intruder would have been readily noticeable to the URE operators on duty and security personnel.

Second, the raised floor and dropped ceilings obscured potential access points, even if an intruder had gained access to the secure facility. Likewise, the data cabling residing in the backup transmission operations center was housed in a continuously-manned controlled access facility and was obscured from view despite the fact that it did not reside within a defined PSP.

Third, although the physical security server logs were not being reviewed, the logs of the associated workstations were being reviewed by an automated logging system, which is configured for automated alerting. As a result, there were measures in place to detect suspicious traffic passing between the servers and the associated workstations.

Fourth, while the workstations used for physical access control and monitoring were not present on URE's master CIP device list, nor covered in the URE recovery plan, the physical security server was on the master CIP device list and was addressed in the URE recovery plan. Thus, the core asset in the URE physical access control scheme was properly designated as a CCA, and readily recoverable following events that might initiate the recovery plan. Additionally, the URE security badging office could only be accessed via controlled access doors and was manned 24 hours a day, seven days a week by URE security personnel, which effectively restricted access to the workstations. Finally, the workstations

were maintained behind perimeter firewalls despite their failure to appear on the master CIP device list.

CIP-007-1 R3.2 (SPP201100608)
CIP-007-1 R3 provides in pertinent part:

> 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).
>
> > R3.2. 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 R3.2 has a "Lower" VRF and a "Severe" VSL.

URE submitted a Self-Report for a violation of CIP-007-1 R3.2. URE had identified security patches applicable to CCAs associated with its EMS which were not installed within the timeframe included in URE's patch management procedure. The required patch installation dates spanned two months and involved applications supporting URE's EMS systems. In total, 1,826 patches were involved over the violation timeframe. Twelve of the uninstalled patches had a high-risk rating, and the remainder of the patches was rated medium-risk. The 12 patches identified by URE as presenting high-risk vulnerabilities were related to specific applications. The patches rated medium-risk were related to various vulnerabilities including: denial-of-service; remote code execution; memory corruption; spoofing; buffer overflow; cross domain security bypass; cross domain information disclosure; http trace; and man-in-the-middle vulnerabilities.

URE self-reported a violation of CIP-007-3 R3.2. URE's vulnerability assessment program required an assessment of all security patches, and the evaluated patches were prioritized as high, medium, low, or waiting on a patch. In one instance, a low-rated patch was not implemented on two CCA physical security servers. Under the existing URE patch management process during the violation timeframe, documentation and implementation of low priority patches was at the discretion of the support engineer/analyst. During the Compliance Audit, the SPP RE Audit Team determined that URE had

acted to prevent future patch installation failures by modifying its process to prohibit patches applicable to CIP-protected Cyber Assets from being assigned a low priority.

During the Compliance Audit, the SPP RE Audit Team found a violation of CIP-007-3 R3.2 because URE had not documented the compensating measures necessary to mitigate risk exposure for two security patches that could not be installed, and one patch that was delayed. In accordance with the URE vulnerability management program, any deviation from a patch installation due date should be documented as an exception and requires the completion and approval of an exception request and the assignment of a revised due date. Additionally, because the installation of the un-installable patches was determined to be technically infeasible, a TFE should have been requested by URE.

SPP RE determined that URE violated CIP-007-1 R3.2 for its failure to implement security patches, failure to document the compensating measures applied to mitigate risk exposure for security patches that could not be installed, and failure to request a TFE where needed.

SPP RE determined the duration of the violation to be from the date of URE's first instance of noncompliance to the date URE completed its Mitigation Plan.

SPP RE determined that the instance of noncompliance identified in the URE Self-Report posed a serious risk to the reliability of the BPS. System patching is critical to maintaining up-to-date systems that are guarded against ever-evolving malicious attack techniques and aid in closing newly discovered vulnerabilities. A failure to update patches timely affects the overall security of cyber systems by increasing the breadth of exposure to cyber threats.

Regarding the risk associated with the patches installed outside the designated installation timeframe, in relation to both the high and medium risk patches. While these patches presented multiple vulnerabilities, the most damaging possible outcomes were all related to the creation of denial-of-service type conditions. A denial-of-service condition affecting systems supporting EMS server capabilities has the potential to render EMS controls and output unavailable during a cyber or physical attack. Such an occurrence could severely restrict the ability of an entity to respond to a real-time emergency. Nevertheless, in this case, no loss of cyber operability occurred.

SPP RE determined that the instances of noncompliance identified in the Self-Report and discovered by the SPP RE Compliance Audit Team, posed a moderate risk to the reliability of the BPS. The risk to the BPS was mitigated by the following factors.

First, the risk to the BPS associated with the low-rated patch was mitigated by the following factors. The patch was designed to close a vulnerability affecting servers utilizing certain services. According to the vulnerability summary, an attacker could exploit the vulnerability by sending a specially-crafted domain name system response to a server running the service. The resulting response by the service could produce a "denial-of-service" incident affecting the implicated CCAs. In this instance of noncompliance, the assets associated with the patch installation failure were used in the control and monitoring of the PSP. SPP RE determined that while a "denial-of-service" attack may have rendered the PSP servers temporarily unavailable, the servers were specifically charged with managing the PSP, and a "denial-of-service" would not have affected the URE EMS or other assets within the ESP. No other assets within the ESP were authorized to receive traffic via the implicated port. Therefore, the resulting risk to the BPS from this instance of noncompliance would have been limited to URE having to control access manually until the servers could be restored.

Second, the risk to the BPS associated with URE's failure to introduce compensating measures for the one delayed patch and the two patches that could not be installed was mitigated by the following factors. The delayed patch related to vulnerabilities which typically are considered by security professionals to present low risk. Further, of the remaining two patches that were not installed, both patches were determined to be technically infeasible for installation. One of the patches would have required an upgrade to a version of a server that had not been approved by the EMS vendor and may have inadvertently compromised the EMS due to incompatibility or conflicting application issues. Additionally, the remaining patch would have to have been uninstalled on the EMS systems, which could have caused other applications relying on the application to fail, thereby compromising interactivity between EMS support applications.

CIP-007-1 R5.2, R5.2.3, R5.3.3 (SPP201100609)

CIP-007-1 R5 provides in pertinent part:

> R5. Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> > R5.2. The Responsible Entity shall implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges including factory default accounts.

****

R5.2.3. 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:

****

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

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

URE self-reported a violation of CIP-007-3 R5.2.3. URE reported that one shared account password for CCA access to its EMS had not been changed within the timeframe included in URE's password management procedure. According to the procedure, shared account passwords should be changed on the date an employee leaves the company. The password change requirement was triggered by the voluntary departure of two employees who no longer required access. The employees utilizing the shared account had administrative-level access to the EMS, which enabled the employees to monitor and control energy management software processes, initiate system start-up/shutdown, and make database changes. Despite electronic access remaining available from the terminal, URE reported that the individuals' physical access was revoked in the required timeframes and no remote access privileges were retained. One of the two individuals at issue was a URE employee who voluntarily retired. The other individual was a contract employee who terminated the contractual relationship to pursue employment with another organization. These individuals' passwords were changed within three months.

URE self-reported a violation of CIP-007-3 R5.2, stating that its processes and procedures for CIP-007-3 R5.2 were non-compliant. During the Compliance Audit, the SPP RE Audit Team reviewed URE's CIP-007-3 R5.2 procedures and determined that the processes and procedures were not compliant. The Audit Team identified a recurring issue across the processes and procedures relating to the securing of the accounts following personnel changes, such as a transfer or termination of employees. URE's

access control procedure states that user IDs needed to be added, removed, modified or disabled according to its procedure related to account management. Accordingly, the Audit Team reviewed the procedures related to account management. The Audit Team determined that URE's shared account process was utilized for maintaining user accounts created by technical services on production devices. Within the document, URE defined "privileged" accounts to be those shared accounts that control services and applications at an operating system level. The document provided that individuals who are in administrator roles and need access to these accounts are considered to be privileged. However, the document failed to specify if "privileged" users alone are allowed to access shared accounts. URE defined "privileged" accounts to be those shared accounts that control services and application at an operating system level. Furthermore, the URE user management systems engineering procedure stated that shared accounts could be used by a variety of types of users, including personnel in transient roles such as training. However, the procedure failed to address the termination of such access except upon the termination of a privileged user. Based on these facts, the SPP RE Audit Team found that URE's procedures failed to state clearly what users could be given shared account access and failed to describe how that access would be revoked in all cases.

During the Compliance Audit, SPP RE Audit Team identified a violation of CIP-007-3 R5.2.3 involving records related to shared account access. The URE shared user account usage was being logged in the form of successful log-in and log-out events, but the log entries did not identify the individual utilizing the shared account. This reduced the accountability surrounding the shared account because URE was not be able to pinpoint the specific user utilizing the shared account at a particular time.

The Audit Team also identified a violation of CIP-007-3 R5.3.3 because the passwords for one EMS user account and one service account had not been changed within the past year. URE subsequently identified that an additional 160 accounts had not undergone annual password changes. SPP RE determined that 67 of those accounts related to administrative level access. The total 162 accounts at issue were all in support of the URE EMS.

SPP RE determined that URE violated: 1) CIP-007-1 R5.2 for its failure to implement processes and procedures related to the securing of the accounts following personnel changes; 2) CIP-007-1 R5.2.3 for its failure to manage the use of shared accounts; and 3) CIP-007-2 R5.3.3 for its failure to change account passwords at least annually.

SPP RE determined the duration of the CIP-007-a R5.2.3 self-reported instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date the shared account password was changed.

SPP RE determined the duration of the CIP-007-3 R5.2 instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date the procedure was updated.

SPP RE determined the duration of the CIP-007-3 R5.2.3 audit-identified instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date a logging and accountability solution was implemented.

SPP RE determined the duration of the CIP-007-3 R5.3.3 audit-identified instance of noncompliance to be from the date the Standard became mandatory and enforceable through upon the implementation of a logging and accountability solution.

SPP RE determined that the aggregate of all instances of noncompliance comprising this violation rose to a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk.

Regarding the risk to the BPS associated with the instances of noncompliance included in the September 30, 2010 Self-Report, URE stated that the two employees' physical access to the CCAs had been revoked within seven calendar days in accordance with CIP-004-1 R4.2. Furthermore, the employees retained no remote access. Additionally, the assets at issue resided within an access-controlled PSP during the pendency of the violation. Therefore, because the access vulnerability was limited to the employee's physical presence at the terminal, the risk of unauthorized access occurring was lowered by URE's preventative controls in place.

Regarding the risk to the BPS associated with the instances of noncompliance included in the Self-Report, SPP RE determined that URE's failure to define all access levels and the procedural requirements for the termination of such access, had the potential effect to negatively impact "segregation of duties" within the environment. Such a failure could result in user-level employees being granted administrative access and retaining such access longer than necessary for completing a job function. This increases the exposure of internal systems to unauthorized access. However, SPP RE determined that URE did have some mitigating preventative and detective controls in place, such as: password change requirements, log reviews, vulnerability analysis, and account revocation following termination.

Regarding the risk to the BPS associated with the instances of noncompliance included in the Audit findings for CIP-007-3 R5.2.3, SPP RE determined that URE's failure to adequately track account users of shared accounts created a risk that URE might not have the ability to identify a malicious insider that utilized the account to harm the URE systems. However, access logs were being maintained, which

would have given indications of what time the access occurred. Furthermore, the shared accounts would have been utilized solely within a 24-hour monitored facility, further reducing a potential malicious insider's anonymity. Additionally, the individuals having access to the implicated Cyber Assets would have undergone Personnel Risk Assessments (PRAs) and Cyber Asset training.

Regarding the risk to the BPS associated with the instances of noncompliance included in the Compliance Audit finding, SPP RE determined that URE's failure to change a substantial number of passwords on at least an annual basis left cyber systems vulnerable to possible attempts from outside the ESP to access systems inside the ESP. However, SPP RE determined that URE's centralized logging reviews would have likely alerted URE to the presence of repeated unauthorized access attempts.

CIP-005-1 R.2.2 and R2.6 (SPP201100610)
CIP-005-1 R2 provides in pertinent part:

> R2. Electronic Access Controls — The Responsible Entity shall implement and document the organizational processes and technical and procedural mechanisms for control of electronic access at all electronic access points to the Electronic Security Perimeter(s).
>
> ****
>
> R2.2. At all access points to the Electronic Security Perimeter(s), the Responsible Entity shall enable only ports and services required for operations and for monitoring Cyber Assets within the Electronic Security Perimeter, and shall document, individually or by specified grouping, the configuration of those ports and services.
>
> ****
>
> 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 R2.2 has a "Medium" VRF and CIP-005-1 R2.6 has a "Lower" VRF. Both Requirements have a "Severe" VSL.

URE self-reported a violation of CIP-005-3 R2.6. URE stated that it had failed to install an appropriate use banner on a pair of Cyber Assets utilized to access the URE ESP. During the Compliance Audit, SPP RE confirmed that the two devices in question did not present a compliant acceptable use banner and that no TFE had been requested by URE.

During the Compliance Audit, SPP RE also determined that URE could not demonstrate that only ports and services required for operations and for monitoring Cyber Assets within the ESP had been enabled as required by CIP-005-1 R2.2. Also, regarding URE's firewall rule sets, the Audit Team determined there was no documentation to demonstrate why any port was enabled. Furthermore, the rule sets for the firewall show that the majority of the rules restrict data traffic to the IP address but do not explicitly permit data traffic at the port level. The traffic between IP addresses should have been limited to specified ports.

SPP RE determined that URE violated CIP-005-1 R2.6 for its failure to install appropriate use banners on a pair of Cyber Assets, and R2.2 for its failure to enable only and services required for operations and for monitoring Cyber Assets.

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

SPP RE determined that this violation posed a minimal risk and did not pose a serious or substantial risk to the reliability of the BPS because the risk was mitigated by several factors. First, only authorized trained personnel would have had physical access to the pair of Cyber Assets lacking an appropriate use banner, thereby minimizing the risk that the devices would be used in an inappropriate method. Second, the failure to document properly why certain ports and services were enabled was mitigated by the fact that URE had additional processes to protect against intrusions, such as automated log review, anti-virus software, and host-level hardening.

CIP-004-3 R2.1, R3, R4.1 and R4.2 (SPP2012009547, SPP2012009983 and SPP2012009760)
CIP-004-3 R2.1, R3, R4.1 and R4.2 provide in pertinent part:

> R2. Training — The Responsible Entity shall establish, document, implement, and maintain an annual cyber security training program for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. The cyber security training program shall be reviewed annually, at a minimum, and shall be updated whenever necessary.

R2.1. This program will ensure that all personnel having such access to Critical Cyber Assets, including contractors and service vendors, are trained prior to their being granted such access except in specified circumstances such as an emergency.

****

R3. Personnel Risk Assessment - The Responsible Entity shall have a documented personnel risk assessment program, in accordance with federal, state, provincial, and local laws, and subject to existing collective bargaining unit agreements, for personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets. A personnel risk assessment shall be conducted pursuant to that program prior to such personnel being granted such access except in specified circumstances such as an emergency.

****

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

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

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

CIP-004-3 R2.1 has a "Medium" VRF and a "Severe" VSL. CIP-004-3 R3 has a "Medium" VRF and a "Severe" VSL. CIP-004-3 R4.1 and R4.2 have a "Lower" VRF and a "High" VSL.

CIP-004-3 R2.1 (SPP2012009547)

URE self-certified non-compliance with CIP-004-3 R2.1. URE stated that as a result of human error, a security officer who assigns keycards inadvertently provided unintended CCA access privileges to two contractors on two separate occasions. Access was inadvertently granted to one contractor for four days, and access was inadvertently granted to another contractor for three days. The contractors had not been trained in accordance with CIP-004-3 R2.1. A bi-weekly, internal URE audit identified the error and access was corrected. The contractors did not attempt to access URE's PSPs or CCAs during the pendency of the violation.

CIP-004-3 R3 (SPP2012009983)

Notwithstanding the fact that the contractors identified in SPP2012009547 did not attempt to access URE's PSPs or CCAs, URE submitted Self-Reports identifying noncompliance with CIP-004-3 R3. URE stated that the two contractors who were inadvertently granted access to URE's CCAs had not received PRAs.

CIP-004-3 R4.1 and R4.2 (SPP2012009760)

URE self-reported a violation of CIP-004-3 R4.2 because it failed to revoke physical and electronic access for one employee within seven calendar days of the employee being transferred. The access revocation was required because the employee was transferred to a different working group where he no longer required access to CCA. The transfer occurred but the employee's electronic and physical access was not revoked until about a month and half later. The electronic and physical access revocation failure stemmed from a lack of staff familiarity with URE's human resources software system. After the employee transfer had been effected, a routine quarterly review of a list of personnel with electronic access was conducted. Through an oversight during the review, the employee's manager failed to identify the employee's active electronic access and have the access removed.

Additionally, URE submitted a Self-Report for a violation of CIP-004-3 R4.1 because it failed to update its list of personnel having CCA access within seven calendar days of the employee transfer.

Similarly, URE self-reported a violation of CIP-004-3 R4.2, stating that it had failed to revoke electronic and physical access to CCAs as required by this Standard. The Help Desk failed to revoke physical and electronic access for 25 days following the receipt of a revocation request. The delay was caused by a submittal for revocation of access that included an incorrect employee ID. As a result of the incorrect ID, the email notification for weekly access review was restricted to one supervisor at the time of the

violation. Following the discovery of this violation, the email is distributed to multiple individuals for review.

SPP RE determined that URE violated CIP-004-3 R2.1 for its failure to ensure that all personnel having authorized cyber or authorized unescorted physical access to CCAs are trained, CIP-004-3 R3 for its failure to ensure that PRAs are conducted according to its PRA program, and CIP-004-3 R4.1 and R4.2 for its failure to review the list of personnel with access to CCAs and to revoke such access within seven calendar days.

SPP RE determined the duration of the first instance of noncompliance for CIP-004-3 R2.1 (SPP2012009547) was from the date the inadvertent granting of access occurred to the date the access was removed. The duration of the second instance of noncompliance was from the date the second inadvertent access grant occurred to the date the second instance of access was removed.

SPP RE determined the duration of the first instance of noncompliance for CIP-004-3 R3 (SPP2012009760) was from the date access was required to be removed to the date access was removed. The duration of the second instance of noncompliance was from the date access was required to be removed to the date access was removed.

SPP RE determined the duration of the first instance of noncompliance for CIP-004-3 R4.2 (SPP2012009983) to be the date the inadvertent access grant occurred to the date the access was removed. The duration of the second instance of noncompliance was from the date the second inadvertent access grant occurred to the date the second instance of access was removed.

CIP-004-3 R2.1 and CIP-004-3 R3 (SPP2012009547, SPP2012009983)

SPP RE determined that the violations of CIP-004-3 R2.1 and CIP-004-3 R3 posed a moderate risk but not a serious or substantial risk to the reliability of the BPS. Specifically, the risk was mitigated by several factors. First, although the contractor at issue should not have been granted access to CCAs, the contractor's access was limited to a maximum of three days in one case and four days in the other case. Also, the contractors never attempted to access the PSP containing the CCAs at issue. Second, granting access to CCAs without conducting a PRA poses a risk that those CCAs may be exposed to personnel presenting a high risk to the CCAs. However, SPP RE determined that the CCAs at issue were located in a facility monitored 24 hours a day, seven days a week by security personnel, thereby reducing the risk to the BPS.

CIP-004-3 R4.1 and R4.2 (SPP2012009760)

SPP RE determined that the violation of CIP-004-3 R4.1 and R4.2 posed a minimal risk and did not pose a serious or substantial risk to the reliability BPS. Despite the failure to revoke access in response to the employee transfers, the employees remained employees of URE following the transfer and continued to be subject to corporate policies supporting Cyber Asset protection. According to its affiliate's records, the employees did not attempt to access any unauthorized PSPs after the date when the access should have been revoked. The employees had no remote access to CCAs, and without entering a 24 hours a day, seven days a week manned and monitored PSP, could not have accessed the CCAs.

CIP-007-3 R 4.1 and R4.2 (SPP2012009592)

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

CIP-007-3 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.
> >
> > 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-007-3 R4.1 and R4.2 have a "Medium" VRF and a "Severe" VSL.

URE self-certified a violation of CIP-007-3 R4, stating that URE discovered that the anti-virus on-access scanner had stopped on some workstations in URE's EMS environment. The cause of the loss of functionality remained undetermined. URE's IT process requires on-access and weekly full-disk scans on individual client computers. However, for the workstations at issue, only the full-disk scans were being performed between two weeks when a system engineer re-enabled the on-access scanner. Additionally, URE discovered that the anti-virus software on one workstation in the EMS/Supervisory Control and Data Acquisition (SCADA) environment was not functioning for approximately two weeks.

SPP RE determined that URE violated CIP-007-3 R4.1 and R4.2 for its failure to implement anti-virus and malware prevention tools and its failure to implement a process for the update of anti-virus and malware prevention "signatures."

SPP RE determined the duration of the first instance of noncompliance to be from the date the on-access scans ceased to the date the on-access scans were re-enabled. The second instance of noncompliance was from the date the anti-virus software ceased working on one URE device to the date the anti-virus software was re-enabled on the device.

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. For approximately two weeks, no anti-virus software was functioning on one EMS device. This failure could have potentially exposed the device to harmful malware that could have used the machine as a gateway to propagate to other devices on the EMS network. However, the risk was mitigated by several factors. First, despite the lack of the on-access scans, weekly full-disk scans were still being run, which would have enabled the detection of malware threats on a weekly basis. Second, the duration of the issue was limited to 11 days on one device, which aided in restricting the potential risk to the EMS network. URE reported that no adverse affects were detected on the URE EMS network during the period of this violation.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of one hundred fifty-three thousand dollars ($153,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. URE's Internal Compliance Program (ICP);
2. The quality of URE's ICP. SPP RE determined that the ICP was not a mitigating factor in the penalty determination due to the fact that, despite a strong culture of self-reporting, several repeat instances of prior non-compliance were identified;

3. URE's violation history, which was considered an aggravating factor in the penalty determination for some of the instant violations;
4. When determining the penalty amount, SPP RE gave credit to URE for the self-reported violations;
5. URE cooperated during the enforcement process, which was considered a mitigating factor in the penalty determination;
6. There was no indication or evidence that URE attempted to conceal the violations; and
7. SPP RE reported that 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 fifty-three thousand dollars ($153,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Status of Mitigation Plans[7]

CIP-003-1 R5.2 (SPP201000425)
URE's Mitigation Plan to address its violation of CIP-003-1 R5.2 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT005062 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update its internal departmental procedures to ensure that all required annual reviews of user access rights to protected information are completed; and
2. Train appropriate personnel on the use of the updated procedures governing access approval and annual review to ensure future reviews encompass all sources containing CCA information.

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

[7] See 18 C.F.R § 39.7(d)(7).

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

CIP-003-1 R6 (SPP201000426)

URE's Mitigation Plan to address its violation of CIP-003-1 R6 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE. The original Mitigation Plan for this violation was designated as MIT-09-3605. The Mitigation Plan was approved by NERC and submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review CIP-003-1 R6 with the employees at issue;
2. Implement a method to visually identify desktop computers as CCAs, thus adding an additional mechanism to alert staff that the asset in question is a CCA;
3. Ensure that all implicated employees had printed copies of the URE Information Security Handbook;
4. Review and update its Information Technology change management process in an effort to increase the documents level of clarity; and
5. Develop, implement, and complete mandatory policy, standard, and process location training for its IT employees.

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

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

CIP-007-1 R4.2 (SPP201000428)

URE's Mitigation Plan to address its violation of CIP-007-1 R4.2 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT005065 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to take the following actions:

1. URE had manually updated all anti-virus signatures on the URE EMS;

2. Manual updates were continued on a bi-weekly basis until the new automated process was implemented;
3. A new automated process was implemented; and
4. After determining the automated process was functioning correctly, URE documented the process.

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

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

CIP-007-1 R9 (SPP201100528)
URE's Mitigation Plan to address its violation of CIP-007-1 R9 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT005071 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Conduct an official review of, and submit for management approval, its malicious software prevention process, and ensure that the formal approval of its access management process was documented. SPP RE determined that the approval of these documents is evidenced in the documents revision history; and
2. Establish an electronic calendar reminder to alert the proper staff of the need to review the malicious software prevention process.

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

After reviewing of URE's submitted evidence, SPP RE verified that URE's Mitigation Plan was completed.

CIP-004-3 R4.1 and R4.2 (SPP201100568)
URE's Mitigation Plan to address its violation of CIP-004-3 R4.1 and R4.2 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 SPPMIT006631 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Initiate the required quarterly review process;
2. Revoke the access of the transferred employee no longer requiring access to CCAs;
3. Update the employee changes section of its access management process to strengthen the language detailing the responsibilities of supervisors and managers in reviewing employee access;
4. Train its supervisors and managers on the updated access management process; and
5. Develop a departmental procedure for personnel access reviews that detailed the steps necessary to ensure quarterly reviews of access rights.

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

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

CIP-005-3 R1 (SPP201100569)

URE's Mitigation Plan to address its violation of CIP-005-3 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 SPPMIT006620 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Remove the ESP access point designation from the supervisory control and data acquisition (SCADA)/EMS communication front-ends on the master CIP Device List;
2. Retire its EMS, thereby integrating its operations under the EMS utilized by its affiliate; and
3. Therefore, the steps taken by URE's affiliate to remediate its violation of CIP-005-1 R1 also remediated URE's violation of CIP-005-3 R1.

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

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

CIP-002-1 R2 (SPP201100604)

URE's Mitigation Plan to address its violation of CIP-002-1 R2 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006553 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Update its restoration plan to include the substation as a Critical Asset; and
2. Ensure that the restoration plan was then approved by the designated senior manager.

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

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

CIP-005-1 R4.2 (SPP201100605)

URE's Mitigation Plan to address its violation of CIP-005-1 R4.2 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 SPPMIT006605 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Document a procedure for reviewing enabled ports and services and include the new procedure in its annual firewall assessment documentation;
2. Perform and document the required review of ports and services; and
3. Develop a method to remind appropriate personnel to review ports and services on an annual basis.

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

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

CIP-006-1 R1.1 and R1.8 (SPP201100607)

URE's Mitigation Plan to address its violation of CIP-006-1 R1.1 and 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 SPPMIT006629 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to take the following actions related to:

1. Router Residing Outside PSP:
    a. Expand the existing PSP to include the URE Telecom room; and
    b. Ensure the application of all applicable NERC CIP Standards to the Telecom room, and designate the area as a PSP.
2. Physical Security Servers:
    a. Identify all CCAs used in physical access control and monitoring;
    b. Apply the NERC CIP Standards to the Cyber Assets used for physical access control and monitoring; and
    c. Add the Cyber Assets used for physical access control and monitoring to the master CIP device List.
3. Data Cable Outside PSPs:
    a. Consolidate the two PSPs connected via the data cabling into one PSP;
    b. Ensure the application of NERC CIP Standards to the newly established PSP; and
    c. Designate the area as a NERC PSP.
4. Recovery Plan:
    a. Update the recovery plan to fully address all CCAs used in the access control and monitoring of the PSPs.
5. Server Logs:

a. Document a procedure requiring and describing the review of the physical access control system logs.

6. Six-wall Boundary:

a. Provide ongoing progress reports for six-wall boundary additions; and

b. Complete all six-wall construction additions and provide a final progress report.

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

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

CIP-007-1 R3.2 (SPP201100608)

URE's Mitigation Plan to address its violation of CIP-007-1 R3.2 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 SPPMIT006630 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Undertake an inter-departmental remediation plan to install all outstanding patches requiring installation;
2. Update its vulnerability management process to restrict patches affecting NERC CIP Cyber Assets to a medium or higher risk rating;
3. Review and revise its information security exception form to require the completion of the compensating measures section prior to submission for approval;
4. Request a TFE for the two sets of patches that could not be implemented; and
5. Hold inter-departmental meetings composed of Information Security, Compliance Operations, and Operations management to highlight the importance of compliance with the vulnerability and exception processes.

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

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

CIP-007-1 R5.2, R5.2.3 and R5.3.3 (SPP201000609)

URE's Mitigation Plan to address its violation of CIP-007-1 R5.2, R5.2.3, and R5.3.3 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006628 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to take the following actions related to:

1. Shared Accounts:
    a. Verified that both employees were removed from password manager; and
    b. Strengthened the EMS access control procedure to reflect additional steps available to secure account passwords.
2. Annual Password Changes:
    a. Modified the passwords for the three user accounts that had not been changed within the past year;
    b. Created and implemented a method to remind appropriate personnel to review password changes for the three user accounts;
    c. Changed passwords on subsequently identified accounts where passwords were not changed within the last year, and set accounts to expire, where technically feasible; and
    d. Submitted TFEs for account passwords that were technically and/or operationally infeasible to change or set to expire.
3. Account Management:
    a. Updated the technical services user management procedure to clarify if only privileged users are permitted access to shared technical services user accounts; and
    b. Updated the system engineering user management procedure to address the revocation of access for personnel in transitional roles.
4. Audit Trail:
    a. Reviewed current methods for shared account usage logging;
    b. Evaluated possible methods for tracking shared account usage;
    c. Designed a method for tracking shared account usage; and

d. Implemented the chosen logging and accountability solution for tracking shared account usage.

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

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

CIP-005-1R2.2 and R2.6 (SPP201100610)
URE's Mitigation Plan to address its violation of CIP-005-1R2.2 and R2.6 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006604 and was submitted as non-public information to FERC in accordance with FERC orders.
URE's Mitigation Plan required URE to:

1. Create an appropriate use banner on the redundant pair of Cyber Assets used for the access control of its EMS's ESP;
2. Hold a review session with the firewall administrators and their manager emphasizing the importance of implementing an appropriate use banner; and
3. Document the firewall rule sets and include comments describing the purpose of each rule.

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

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

CIP-004-3 R2.1; R3; and R4.1 and R4.2 (SPP2012009547, SPP2012009983 and SPP2012009760)
URE's Mitigation Plan to address its violation of CIP-004-3 R2.1 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007953-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-004-3 R3 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this

violation is designated as SPPMIT007956-1and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan to address its violation of CIP-004-3 R4.1 ad R4.2 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007955-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to:

1. Document a physical security procedure requiring a secondary peer review when access is being granted to a PSP;
2. Train relevant staff on the peer review procedure, and implement the peer review procedure;
3. Modify its system to list the NERC PSP access choices across the bottom of the selection screen;
4. Hold a refresher training session with the Human Resources personnel responsible for updating NERC Compliance related personnel job data in the Human Resources system;
5. Update its Human Resources program to accept employee job data changes regardless of the order in which the data is saved; and
6. Add physical and cyber access control compliance responsibilities information to its required annual employee information security training.

URE certified that the above Mitigation Plan SPPMIT007953-1 was completed. URE submitted evidence of completion of its Mitigation Plan.

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan SPPMIT007953-1 was completed.

URE certified that the above Mitigation Plan SPPMIT007956-1 was completed. URE submitted evidence of completion of its Mitigation Plan.

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan SPPMIT007956-1 was completed.

URE certified that the above Mitigation Plan SPPMIT007955-1 was completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan SPPMIT007955-1 was completed.

CIP-007-3 R4.1 and R4.2 (SPP2012009592)
URE's Mitigation Plan to address its violation of CIP-007-3 R4.1 and R4.2 was submitted as complete to SPP RE. The Mitigation Plan was accepted by SPP R and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007954-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plans required URE to repair the anti-virus connection on its EMS system, which was then retired.

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

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan for this violation was completed.

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

Basis for Determination

Taking into consideration the Commission's direction in Order No. 693, the NERC Sanction Guidelines and the Commission's July 3, 2008, October 26, 2009 and August 27, 2010 Guidance Orders,[9] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on December 10, 2012. The NERC BOTCC approved the Settlement Agreement, including SPP RE's assessment of a one hundred fifty-three thousand dollar ($153,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In

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

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 Internal Compliance Program (ICP);
2. The quality of URE's ICP. SPP RE determined that the ICP was not a mitigating factor in the penalty determination;
3. URE's violation history, which was considered an aggravating factor in the penalty determination for some of the instant violations;
4. URE self-reported some of the violations, as discussed above;
5. URE cooperated during the enforcement process, which was considered a mitigating factor in the penalty determination;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. SPP RE reported that there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred fifty-three thousand dollars ($153,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

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

Request for Confidential Treatment

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

Entity sensitive business information and confidential information regarding critical energy infrastructure.

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

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

Attachments to be Included as Part of this Notice of Penalty

a) Settlement Agreement by and between SPP RE and URE executed December 27, 2012, included as Attachment a;

1. SPP RE's Disposition of Violation: Information Common to Instant Violations, included as Attachment A to the Settlement Agreement;
2. SPP RE's Disposition of Violation for CIP-003-1 R5.2, SPP201000425, included as Attachment B to the Settlement Agreement;
3. SPP RE's Disposition of Violation for CIP-003-1 R6, SPP2010100426, included as Attachment C to the Settlement Agreement;
4. SPP RE's Disposition of Violation for CIP-007-1 R4.2, SPP201000428, included as Attachment D to the Settlement Agreement;
5. SPP RE's Disposition of Violation for CIP-007-1 R9, SPP201100528, included as Attachment E to the Settlement Agreement;
6. SPP RE's Disposition of Violation for CIP-004-3 R4.1 and R4.2, SPP201100568, included as Attachment F to the Settlement Agreement;
7. SPP RE's Disposition of Violation for CIP-005-1 R1, SPP201100569, included as Attachment G to the Settlement Agreement;
8. SPP RE's Disposition of Violation for CIP-002-1 R2, SPP201100604, included as Attachment H to the Settlement Agreement;
9. SPP RE's Disposition of Violation for CIP-005-1 R4.2, SPP201100605, included as Attachment I to the Settlement Agreement;

10. SPP RE's Disposition of Violation for CIP-006-1 R1.1 and R1.8, SPP201100607, included as Attachment J to the Settlement Agreement;
11. SPP RE's Disposition of Violation for CIP-007-1 R3.2, SPP201000608, included as Attachment K to the Settlement Agreement;
12. SPP RE's Disposition of Violation for CIP-007-1 R5.2, R5.2.3, R5.3.3, SPP201100609, included as Attachment L to the Settlement Agreement;
13. SPP RE's Disposition of Violation for CIP-004-3 R2.1, R3, R4.1 and R4.2, SPP2012009547, SPP2012009760 and SPP2012009983, included as Attachment M to the Settlement Agreement;
14. SPP RE's Disposition of Violation for CIP-005-1 R2.2 and R2.6, SPP201100610, included as Attachment N to the Settlement Agreement;

b) Record documents for the violations of CIP-003-1 R5.2, SPP201000425, included as Attachment b:
   1. URE's Self-Report for SPP201000425;
   2. URE's Mitigation Plan for SPP201000425 designated as SPPMIT005062;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

c) Record documents for the violations of CIP-003-1 R6, SPP2010100426, included as Attachment c:
   1. URE's Self-Report for SPP2010100426;
   2. URE's Mitigation Plan for SPP2010100426 designated as MIT-09-3605;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

d) Record documents for the violations of CIP-007-1 R4.2, SPP201000428, included as Attachment d:
   1. URE's Self-Report for SPP201000428;
   2. URE's Mitigation Plan for SPP201000428 designated as SPPMIT005065;
   3. URE's Certification of Mitigation Plan Completion; and
   4. SPP RE's Verification of Mitigation Plan Completion.

e) Record documents for the violations of CIP-007-1 R9, SPP201100528, included as Attachment e:
   1. URE's Self-Report for SPP201100528;

2. URE's Mitigation Plan for SPP201100528 designated as SPPMIT005071;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

f) Record documents for the violations of CIP-004-3 R4.1 and R4.2, SPP201100568, included as Attachment f:

1. URE's Self-Report for SPP201100568;
2. URE's Self-Report for SPP201100568;
3. URE's Mitigation Plan for SPP201100568 designated as SPPMIT006631;
4. URE's Certification of Mitigation Plan Completion; and
5. SPP RE's Verification of Mitigation Plan Completion.

g) Record documents for the violations of CIP-005-1 R1, SPP201100569, included as Attachment g:

1. URE's Self-Report for SPP201100569;
2. SPP RE's Source document for SPP201100569;
3. URE's Mitigation Plan for SPP201100569 designated as SPPMIT006620;
4. URE's Certification of Mitigation Plan Completion; and
5. SPP RE's Verification of Mitigation Plan Completion.

h) Record documents for the violations of CIP-002-1 R2, SPP201100604, included as Attachment h:

1. SPP RE's Source document for SPP201100604 (see Attachment g-2);
2. URE's Mitigation Plan for SPP201100604 designated as SPPMIT006653;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

i) Record documents for the violations of CIP-005-1 R4.2, SPP201100605, included as Attachment i:

1. SPP RE's Source document for SPP201100605 (see Attachment g-2);
2. URE's Mitigation Plan for SPP201100605 designated as SPPMIT006605;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

j) Record documents for the violations of CIP-006-1 R1.1 and R1.8, SPP201100607, included as Attachment j:

1. URE's Self-Report for SPP201100607;
2. SPP RE's Source document SPP201100607 (see Attachment g-2);
3. URE's Mitigation Plan for SPP201100607designated as SPPMIT006629;
4. URE's Certification of Mitigation Plan Completion; and
5. SPP RE's Verification of Mitigation Plan Completion.

k) Record documents for the violations of CIP-007-1 R3.2, SPP201000608, included as Attachment k:

1. URE's Self-Report for SPP201000608;
2. URE's Self-Report for SPP201000608;
3. SPP RE's Source document for SPP201000608 (see Attachment g-2);
4. URE's Mitigation Plan for SPP201000608 designated as SPPMIT006630;
5. URE's Certification of Mitigation Plan Completion; and
6. SPP RE's Verification of Mitigation Plan Completion.

l) Record documents for the violations of CIP-007-1 R5.2, R5.2.3, R5.3.3, SPP201100609, included as Attachment l:

1. URE's Self-Report for SPP201100609;
2. URE's Self-Report for SPP201100609;
3. SPP RE's Source document for SPP201100609 (see Attachment g-2);
4. URE's Mitigation Plan for SPP201100609 designated as SPPMIT006628;
5. URE's Certification of Mitigation Plan Completion; and
6. SPP RE's Verification of Mitigation Plan Completion.

m) Record documents for the violations of CIP-005-1 R2.2 and R2.6, SPP201100610, included as Attachment m:

1. URE's Self-Report for SPP201100610;
2. SPP RE's Source document for SPP201100610 (see Attachment g-2);

3. URE's Mitigation Plan for SPP201100603 designated as SPPMIT006604;
4. URE's Certification of Mitigation Plan Completion; and
5. SPP RE's Verification of Mitigation Plan Completion.

n) Record documents for the violations of CIP-007-3 R4.1 and R4.2, SPP2012009592, included as Attachment o:

1. URE's Self-Report for SPP2012009592;
2. URE's Mitigation Plan for SPP2012009592 designated as SPPMIT007954-1 submitted;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

o) Record documents for the violations of CIP-004-3 R2.1, R3, R4.1 and R4.2, SPP2012009547, SPP2012009760 and SPP2012009983, included as Attachment o:

1. URE's Self-Report for SPP2012009547;
2. URE's Self-Report for SPP2012009983;
3. URE's Self-Report for SPP2012009760;
4. URE's Self-Report for SPP2012009760;
5. URE's Mitigation Plan for SPP2012009547 designated as SPPMIT007953-1;
6. URE's Mitigation Plan for SPP2012009760 designated as SPPMIT007956-1;
7. URE's Mitigation Plan for SPP2012009983 designated as SPPMIT007955-1;
8. URE's Certification of Mitigation Plan Completion for SPP2012009547;
9. SPP RE's Verification of Mitigation Plan Completion for SPP2012009547;
10. URE's Certification of Mitigation Plan Completion for SPP2012009760;
11. SPP RE's Verification of Mitigation Plan Completion for SPP2012009760;
12. URE's Certification of Mitigation Plan Completion for SPP2012009983; and
13. SPP RE's Verification of Mitigation Plan Completion for SPP2012009983.

A Form of Notice Suitable for Publication[10]

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

[10] *See* 18 C.F.R § 39.7(d)(6).

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

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net Ron Ciesiel* General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (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.	Rebecca J. Michael* Associate General Counsel for Corporate and Regulatory Matters Meredith May Jolivert* Attorney North American Electric Reliability Corporation 1325 G Street, N.W. Suite 600 Washington, DC 20005-3801 (202) 644-8052 (202) 644-8099 – facsimile rebecca.michael@nerc.net meredith.jolivert@nerc.net Peggy Lewandoski* Paralegal & SPP RE File Clerk Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 482-2057 (501) 482-2025 – facsimile spprefileclerk@spp.org Joe Gertsch* Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1672 (501) 482-2025 – facsimile jgertsch.re@spp.org

Conclusion

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

Respectfully submitted,

/s/ Rebecca J. Michael

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

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

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

cc: The Southwest Power Pool Regional Entity
Unidentified Registered Entity

Attachments