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-007-1 R9, CIP-003-3 R6, CIP-007-3 R1.1, CIP-004-3 R4.2, CIP-005-1 R1, CIP-002-1 R2, CIP-005-1 R4.2, CIP-006-1 R1, CIP-007-1 R3.2, CIP-007-1 R5, CIP-007-1 R6.5, CIP-004-3 R2.1, CIP-004-3 R4, CIP-004-3 R3, and CIP-007-3 R5.1.1. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of one hundred seven thousand dollars ($107,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the Settlement Agreement. Accordingly, the violations identified as NERC Violation Tracking Identification

[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.

Numbers SPP201000421, SPP201100526, SPP201100535, SPP201100536, SPP201100557, SPP201100558, SPP201100596, SPP201100598, SPP201100600, SPP201100601, SPP201100602, SPP201100603, SPP2012009554, SPP2012009762, SPP2012009984, and SPP2012010535 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-1716	SPP201000421	CIP-003-1	R5.2	Lower	$107,000
			SPP201100526	CIP-007-3	R9	Lower	
			SPP201100535	CIP003-3	R6	Lower	
			SPP201100536	CIP-007-3	R1.1	Medium	
			SPP201100557	CIP-004-3	R4.2	Lower	
			SPP201100558	CIP-005-1	R1	Medium	
			SPP201100596	CIP-002-1	R2	Lower	
			SPP201100598	CIP-005-1	R4.2	Medium	

			SPP201100600	CIP-006-1	R1.1, R1.8	Medium; Lower	
			SPP201100601	CIP-007-1	R3.2	Lower	
			SPP201100602	CIP-007-1	R5.1.1, R5.2, R5.2.3, R5.3.3	Lower; Lower; Medium; Medium	
			SPP201100603	CIP-007-1	R6.5	Lower	
			SPP2012009554	CIP-004-3	R2.1	Medium	
			SPP2012009762	CIP-004-3	R4.1, R4.2	Lower	
			SPP2012009984	CIP-004-3	R3	Medium	
			SPP2012010535	CIP-007-3	R5.1.1	Lower	

CIP-003-1 R5.2 (SPP201000421)

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 R5.2 provides in pertinent part:

> R5. Access Control - The Responsible Entity[4] shall document and implement a program for managing access to protected Critical Cyber Asset information.
>
> > R5.2 The Responsible Entity shall review at least annually the access privileges to protected information to confirm that access privileges are correct and that

[4] 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.

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 correctly assigned and correspond with 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 to 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) because 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.

CIP-007-3 R9 (SPP201100526)

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-007-3 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 thirty 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 an 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 documented final approval. 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 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 documents for a final review, no substantive changes were made to the documents during the review phase. Additionally, the prior year's review approved versions of both the malicious software prevention document and access management document were still in active use with no loss of URE 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-003-3 R6 (SPP201100535)

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

CIP-003-3 R6[5] provides:

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

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

URE self-reported a violation of CIP-003-1 R6 regarding the execution of a change control and configuration management process for CCAs. Although a change control and configuration 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.

URE self-reported an additional instance of noncompliance with CIP-003-3 R6 because URE had failed to follow its documented change control and configuration management procedure for software additions on CCAs. Specifically, installation of software occurred on three Cyber Assets but the installations were inconsistent with the established change management procedure. According to URE, the installation technician was unaware that the Cyber Assets in question were designated CCAs, and installed the system updates to allow the operation of some utilities related to applications. The assets at issue were consoles used to connect operators to URE's EMS. Following the discovery of the installation technician's failure to adhere to the change management process, URE removed the software from the affected Cyber Assets. The software was installed for five days on one Cyber Asset and for one day on the remaining two Cyber Assets.

URE reported another instance of noncompliance with CIP-003-3 R6. A virtual device residing on an existing server was powered on inside an electronic security perimeter (ESP) without obtaining the preliminary approval or undergoing preliminary testing, as required by URE's change control process. URE's Information Technology staff was immediately alerted by URE's configuration compliance

[5] The purpose of Reliability Standard CIP-003-3 is the same as the one stated above for CIP-003-1.

manager and vulnerability scanner that the device had been powered on. The device was successfully tested and moved outside of the ESP two months later.

SPP RE determined that URE violated CIP-003-3 R6 for its failure follow its change control and configuration management process.

SPP RE determined the duration of the first instance of noncompliance to be the date the Standard became mandatory and enforceable, through the date URE completed its Mitigation Plan. The second instance of noncompliance was from the date the first Patch was installed outside of change control through the date the patches were removed. The third instance of noncompliance was from the date the device was powered on outside of change control procedures through the date the device was moved outside the ESP.

SPP RE determined that the first instance of noncompliance self-reported, 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, although URE lacked some documentation to evidence its change control and configuration management 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 is submitted to department supervisors or project sponsors, if the change is requested by the business division, and finally to a board for review and scrutiny. The board is responsible for governance of URE's Information Technology division. Second, board approvals had been received where a change had been requested during the violation period, thereby reducing the risk to the BPS.

SPP RE determined that the second instance of noncompliance self-reported posed a minimal risk and did not pose a serious or substantial risk to the reliability of BPS because URE's client configuration manager management server properly identified and alerted URE information security personnel of the installation occurring outside of change control, and the security personnel promptly uninstalled the implicated software. System status logs were also checked and there were no changes to URE's capability to monitor or control the transmission system, and no compromises to the security of URE's Cyber Assets, resulting from the non-compliant installation method. Additionally, the software patches were all identified and removed within a five-day timeframe.

SPP RE determined that the third instance of noncompliance self-reported posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The activation of the device

within the ESP had the potential to introduce unknown vulnerabilities into the ESP. Because the device had not been tested in accordance with the change control procedures, potential software issues could have compromised other devices within the ESP, which could have adversely affected URE's EMS. However, the risk was mitigated by the fact that URE's vulnerability scanner immediately alerted staff to the activation of the device outside of change control. This allowed staff to quickly respond to the device activation. Additionally, no adverse impacts were experienced as a result of the activation.

CIP-007-3 R1.1 (SPP201100536)

CIP-007-3[6] R1.1 provides:

> R1. Test Procedures - The Responsible Entity shall ensure that new Cyber Assets and significant changes to existing Cyber Assets within the Electronic Security Perimeter do not adversely affect existing cyber security controls. For purposes of Standard CIP-007-3, a significant change shall, at a minimum, include implementation of security patches, cumulative service packs, vendor releases, and version upgrades of operating systems, applications, database platforms, or other third-party software or firmware.
>
> R1.1 - The Responsible Entity shall create, implement, and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

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

URE self-reported a violation of CIP-007-3 R1.1 because it had failed to test software updates applicable to CCAs prior to installation. According to URE, the installation technician was unaware that the Cyber Assets were designated CCAs and installed the system updates to allow the operation of some utilities related to applications. The CCAs at issue were consoles used to connect operators to the URE's EMS. Following discovery of the failure to test the software updates, URE removed the software from the affected CCAs. The software was installed for five days on one CCA and for one day on two CCAs.

URE self-reported an additional instance of noncompliance with CIP-007-3 R1.1 because it failed to test a software update to its EMS servers prior to installation of the update. URE uninstalled a prior antivirus version and installed an updated version According to URE, the system engineer performing

[6] The purpose of Reliability Standard CIP-007-3 is the same as the one stated above for CIP-007-1.

the upgrade neglected to check URE's master list of CCAs prior to performing the upgrades and was unaware that two of the devices upgraded were CCAs.
SPP RE determined that URE violated CIP-007-3 R1.1 because it failed to implement and maintain cyber security test procedures in a manner that minimizes adverse effects on the production system or its operation.

SPP RE determined the duration of the first instance of noncompliance to be from the date of the initial noncompliant software installations to the date all noncompliant software installations were removed. The duration of the second instance of noncompliance was from the date of the subsequent noncompliant software installation to the date the software installation was appropriately documented and tested within 24 hours.

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. Regarding the installation, URE's client configuration manager management server properly identified and alerted URE information security personnel that the installation had occurred without the required testing, and the security personnel promptly uninstalled the implicated software. The updates involved well-known software, which is part of regular software updates across multiple types of software, and the updates had never caused operational issues on the URE CCAs. System status logs were also checked and it was determined that the updates did not reduce URE's capability to monitor or control the transmission system. The noncompliant installation of the updates did not compromise the security of URE's Cyber Assets. Finally, the software patches were all identified and removed within five days.

Regarding the second installation, the change was appropriately documented according to URE procedure and a cyber security control test was completed by information security personnel within 24 hours of the upgrade. The upgrade was from a trusted vendor, and the prior software version had functioned properly without compromising the EMS. Finally, the cyber security control test found no issues to be remediated.

CIP-004-3 R4.2 (SPP201100557)
The purpose statement of Reliability Standard CIP-004-3 provides: "Standard CIP-004-3 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004-3 should be read as part of a group of standards numbered Standards CIP-002-3 through CIP-009-3."

CIP-004-3 R4 provides in pertinent part:

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

URE self-reported a violation of CIP-004-3 R4.2. URE failed to remove within the required seven-day timeframe the access of one EMS engineer when the engineer 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 about two and half months later.

SPP RE determined that URE violated CIP-004-3 R4.2 for its failure to revoke access to CCAs within seven calendar days for personnel who no longer require such access to CCAs.

SPP RE determined the duration of the violation to be 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 and did not pose a serious or substantial risk to the reliability of the BPS because the transferred employee was not terminated for cause and remained an employee of URE. Also, the employee had completed cyber security training and had a Personnel Risk Assessment (PRA). URE did not identify any unauthorized access by the employee following the date when the access revocation should have occurred.

CIP-005-1 R1 (SPP201100558)

The purpose statement of Reliability Standard CIP-005-1 provides in pertinent part: "Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical

Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009."

CIP-005-1 R1 provides 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 the 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 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. The first instance of noncompliance involved a failure to identify the proper access point, and despite this identification failure, the device in question 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 (SPP201100596)

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

CIP-002-1 R2 provides:

Critical Asset Identification — The Responsible Entity 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 of URE, SPP RE determined that URE failed to identify one of its substations as a Critical Asset. The substation is in the electrical path of transmission lines used for initial system restoration as provided in the URE System Restoration Plan. CIP-002-1 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 URE's 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 its 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. As a result, URE failed to

include the substation on its list of identified Critical Assets determined through an annual application of its RBAM.

SPP RE determined that URE violated CIP-002-1 R2 for its failure to 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. Additionally, URE has redundancies built into the blackstart portion of URE's system restoration plan. The URE 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 a 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 (SPP201000598)

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 of URE, 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 (SPP201100600)

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"

CIP-006-1 R1 provides in pertinent part:

> 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.

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.

In a second Self-Report, URE identified an additional instance of noncompliance with CIP-006-3c R2 because prior to a certain time, 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 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; 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; 3) ensure that the network data cables between two of URE's PSPs were enclosed within a "six-wall" boundary; and 4) include all Cyber Assets used for physical access control and monitoring in URE's master CIP device list.

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 R1.8 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 related (master CIP device list) 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 did 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's 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. Additionally, the workstations were maintained behind perimeter firewalls despite their failure to appear on the master CIP device list.

CIP-007-1 R3.2 (SPP201000601)

CIP-007-1 R3.2 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 approximately a year 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 had a violation of CIP-007-1 R3.2 for its failure to: 1) implement security patches; 2) document the compensating measures applied to mitigate risk exposure for security patches that could not be installed; and 3) 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. While the 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 R5.1.1 R5.2, R5.2.3, and R5.3.3 (SPP201100602)

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.
>
> R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed
>
> R5.1.1. The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003 Requirement R5.
>
> ****
>
> R5.2. 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 possible violation of CIP-007-3 R5.1.1, stating that it had discovered an account established on a Cyber Asset prior to the CIP standards becoming effective. The account at issue was not granted in conformance with URE's CIP account management requirements. URE confirmed that the account was enabled on a dedicated workstation supporting the operations map board. URE determined that the account was no longer required and removed it. Additionally, during the first quarter, an additional account was added to the map board workstation. That account was detected during account reviews and removed after a determination that the account was unnecessary.

URE self-reported a violation of CIP-007-3 R5.2.3. URE reported that three shared account passwords for CCA access to its EMS had not been changed within the timeframe included in the URE password management procedure. According to the procedure, shared account passwords should be changed on the date an employee leaves the company. URE failed to change the three shared account passwords for its EMS when two employees voluntarily left the company on two separate occasions. The two employees utilizing the shared accounts had administrative level access to the EMS, which enabled them 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 indicated that the two individuals' physical access was revoked in the required timeframes and no remote electronic 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 its 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 users IDs needed to be removed, added, 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 stated that 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's user management systems 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 clearly state what users could be given shared account access and failed to describe how that access would be revoked in all cases.

During the same SPP's Compliance Audit, SPP RE Audit Team identified a violation of CIP-007-3 R5.2.3 involving records relating 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 reduces the accountability surrounding the shared account because URE would not be able to pin-point 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 three user account passwords (one service account for URE's vulnerability management tool, and two URE EMS accounts) had not been changed within the past year. URE subsequently identified that an additional 166 accounts had not undergone annual password changes. SPP RE determined that 19 of those accounts related to administrative level access. The total 169 accounts at issue were all in support of the URE EMS.

SPP RE determined that URE violated: 1) CIP-007-1 R5.1.1 for its failure to remove an account that was no longer required at the time; 2) CIP-007-1 R5.2 for its failure to implement a policy to minimize and manage the scope and acceptable use of administrator, shared, and other generic account privileges; 3) CIP-007-1 R5.2.3 for its failure to manage the use of shared accounts in a way that would identify the specific user at any time; and 4) CIP-007-2 R5.3.3 for its failure to change three account passwords at least annually.

SPP RE determined the duration of the CIP-007-1 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-007-1 R5.1.1 instance of noncompliance to be from the date the Standard became mandatory and enforceable through the date the unnecessary account was removed.

SPP RE determined the duration of the CIP-007-1 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 when the 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 when the logging and accountability solution was implemented.

SPP RE determined that the aggregate of all instances 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 instance of noncompliance included in the Self-Report, URE stated that the two implicated 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 instance of noncompliance included in the Self-Report of CIP-007-3 R5.1.1, the failure to remove the accounts from the map board workstation presented a minimal-risk to the EMS environment. The map board, while aiding in real-time awareness of system events, was not a Critical Asset because the same information was available via the EMS operator terminals. Therefore, any potential sabotage of the specific asset would not have limited real-time awareness. Furthermore, anyone having access to the system would have had to enter the EMS PSP via a controlled access entryway. Only authorized individuals had such physical access.

Regarding the risk to the BPS associated with the instance of noncompliance included in the Self-Report, SPP RE determined that URE's failure to adequately define all access levels and the procedural requirements for the termination of such access, has the potential effect to negatively impact "segregation of duties" within the environment. Such a failure would 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.

Regarding the risk to the BPS associated with the instance of noncompliance included in the Audit finding for CIP-007-3 R5.2.3, SPP RE determined that URE's failure to adequately track account users of shared accounts creates 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 account 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 Cyber Assets would have had undergone a PRA and Cyber Asset training.

Regarding the risk to the BPS associated with the instances of noncompliance included in the Audit finding related to URE's failure to change account passwords annually, the 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-007-1 R6.5 (SPP201100603)
CIP-007-1 R6.5 provides:

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

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

CIP-007-1 R6.5 has a "Lower" VRF and a "Severe" VSL.

During the Compliance Audit, SPP RE identified a violation of CIP-007-3 R6.5 related to the implementation and review of automated tools and organizational process controls to monitor system events. SPP RE determined that URE could not produce evidence to demonstrate that it had reviewed certain logs. Nevertheless, URE asserted that it was conducting reviews of the logs despite the lack of documentation substantiating such reviews. Security events effecting the associated application were

written to the logs, which were stored outside of URE's log management and analysis system, utilized to conduct electronic log reviews. Therefore, URE asserted that the logs had to be reviewed in a different manner. URE could not demonstrate that such reviews had taken place. The logs are required to be periodically reviewed and the reviews should be documented under this Standard.

SPP RE determined that URE violated CIP-007-1 R6.5 for its failure to review logs of system events related to cyber security and maintain records documenting review of logs.

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 because the risk was mitigated by the following factors. URE's failure to review the logs might lead to the failure to detect malicious connection requests. The risk involves the possibility that attacks, which did not progress into the database, might not be identified, and additionally, that unauthorized changes might occur inside the database. However, SPP RE determined that any potential attacks would have to bypass the review of firewall logs. The daily 24 hour analysis of the data traffic through the firewall reduced the risk that a malicious attack could actually reach the associated application without detection.

CIP-004-3 R2.1, R3, R4.1 and R4.2 (SPP2012009554, SPP2012009984, and SPP2012009762)
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 (SPP2012009554)

URE self-certified that it was non-compliant 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 a contractor. The contractor had not been trained in accordance with CIP-004-3 R2.1. A bi-weekly, URE internal Audit identified the error and access was corrected within four days of the discovery of the violation. The contractor did not attempt to access URE PSPs or CCAs during the pendency of the violation.

CIP-004-3 R3 (SPP2012009984)

Notwithstanding the fact that the contractor identified in the violation of CIP-004-3 R2.1, did not attempt to access URE's PSPs or CCAs, URE submitted a Self-Report for CIP-004-3 R3. URE stated that

the contractor which was inadvertently granted access to URE CCAs, had not received a PRA, as required by CIP-004-3 R3.

CIP-004-3 R4.1 and R4.2 (SPP2012009762)

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 CCAs. The transfer occurred but, the employee's electronic and physical access was not revoked until a month and a 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 transferred, 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 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 of a transferred employee for 25 days following the transfer. As a result of an incorrect employee ID on the submittal for access revocation, the email notification for weekly access review was not routed to the appropriate supervisor.

SPP RE determined that URE violated CIP-004-3 R2.1 for a failure to ensure that all personnel having authorized cyber or authorized unescorted physical access to CCAs are trained, CIP-004-3 R3 for a failure to ensure that a PRA is 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 days.

SPP RE determined the duration of the violation of CIP-004-3 R2.1 (SPP2012009554) to be from the date the inadvertent access grant occurred to the date the access was removed. The duration of the violation of CIP-004-3 R3 (SPP2012009984) was from the date the inadvertent access grant occurred through the date the access was removed.

The duration of the first instance of noncompliance for CIP-004-3 R4.1 and R4.2 (SPP2012009762) to be from the date access was required to be removed under the Standard to the date access was removed. The duration of the second instance of noncompliance was from the date access was required to be removed under the Standard to the date access was removed.

CIP-004-3 R2.1 and CIP-004-3 R3 (SPP2012009554, SPP2012009984)

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 employee's access was limited to a maximum of three days, and the employee never attempted to access the PSP containing the CCAs at issue. Second, granting access to CCAs without conducting a PRA poses the 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 (SPP2012009762)

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 URE corporate policies supporting Cyber Asset protection. According to URE'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 R5.1.1 (SPP2012010535)

CIP-007-3 R5.1.1 provides:

> Account Management — The Responsible Entity shall establish, implement, and document technical and procedural controls that enforce access authentication of, and accountability for, all user activity, and that minimize the risk of unauthorized system access.
>
> R5.1. The Responsible Entity shall ensure that individual and shared system accounts and authorized access permissions are consistent with the concept of "need to know" with respect to work functions performed.
>
> R.5.1.1 The Responsible Entity shall ensure that user accounts are implemented as approved by designated personnel. Refer to Standard CIP-003-3 Requirement R5.

CIP-007-3 R5.1.1 has a "Lower" VRF and a "Severe" VSL.

URE self-reported a violation of CIP-007-3 R5.1.1 related to account management. An authorization request was submitted to URE's system engineering division to create a generic domain account. The system engineering division inadvertently created the account in a CIP production domain on a CCA without the review and approval of the information asset owner. Four days later, during an internal audit of electronic and physical access to CCAs, it was discovered that the account was in the CIP production domain. Subsequently, system engineering deleted the account from the CIP production domain and added it to a non-CIP production domain. Because system engineering did not follow its division process and department procedure, which required information asset owners to review and approve requests to create generic accounts, URE failed to comply with CIP-007-3 R5.1.1.

SPP RE determined that URE had violated CIP-007-3 R5.1.1 for a failure to ensure that all user accounts are implemented as approved by designated personnel.

SPP RE determined the duration of the violation to be from the date the noncompliant account was created to the date the account was deleted.

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 there was no record of the account being accessed during the violation period, and the domain on which the account was installed did not contain the necessary software to make the account meaningful. In addition, had access occurred, the data available to the account user was not BPS-sensitive information, thereby reducing the risk to minimal.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of one hundred seven thousand dollars ($107,000) 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 seven thousand dollars ($107,000) 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 (SPP201000421)
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 SPPMIT005058 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.

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

[7] *See* 18 C.F.R § 39.7(d)(7).

CIP-007-1 R9 (SPP201100526)

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 SPPMIT005069 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. 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-003-3 R6 (SPP201100535)

URE's Mitigation Plan to address its violation of CIP-003-3 R6 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT007952-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Review Standard 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 Information Technology 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-007-3 R1.1 (SPP201100536)
URE's Mitigation Plan to address its violation of CIP-007-3 R1.1 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 SPPMIT007946-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Ensure that the employee submitting the request for the system upgrades was forwarded a copy of the most current Master CIP device list; and
2. Update its change management process to clarify the timeframe in which a cyber security controls test must be completed for emergency changes.

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

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

CIP-004-3 R4.2 (SPP201100557)
URE's Mitigation Plan to address its violation of CIP-004-3 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 SPPMIT006556 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Revoke the access of the employee no longer requiring access to CCAs;
2. Update the employee changes section of its access management process document to strengthen the language detailing the responsibilities of supervisors and managers in reviewing employee access; and
3. Train its supervisors and managers on the updated access management 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-005-1 R1 (SPP201100558)

URE's Mitigation Plan to address its violation of CIP-005-1 R1 was submitted to SPP RE. The Mitigation Plan was accepted by SPP RE and approved by NERC. The Mitigation Plan for this violation is designated as SPPMIT006608 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) and EMS communication front-ends on its master CIP device list;
2. Identify and documented its signal switching device as the electronic access points where serial protocol traffic from the RTUs in the field enter the ESP and connect to the EMS front-end; and
3. Diagram appropriately diagramed the configuration described above.

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 R2.4 (SPP201100596)

URE's Mitigation Plan to address its violation of CIP-002-1 R2.4 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 SPPMIT006552 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 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 (SPP201100598)
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 SPPMIT006607 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 documented 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 (SPP201100600)
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 SPPMIT006634 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. 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 URE's master CIP device List.
2. 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.
3. Recovery Plan:
    a. Update the recovery plan to fully address all CCAs used in the access control and monitoring of the PSPs.
4. Server Logs:
    a. Document a procedure requiring and describing the review of the physical access control system logs.
5. 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 (SPP201100601)

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 SPPMIT006635 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;[8] 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 on. 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 R5.1.1, R5.2, R5.2.3, and R5.3.3 (SPP201000602)

URE's Mitigation Plan to address its violation of CIP-007-1 R5.1.1, 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 SPPMIT006636 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:

[8] The TFEs were accepted by SPP RE.

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. User Accounts

a. Verified current domain groups and group membership;

b. Ensured the list of domain groups produced for the third quarter quarterly audit lists actual names of domain groups rather than solely the identification number; and

c. Communicated with IT managers and supervisors regarding the items to be reviewed during quarterly user access audits including the review of domain groups, members of the domain groups, and names of the domain groups rather than solely the identification number.

4. 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.

5. 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. As evidence of completion of its Mitigation Plan, 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 R6.5 (SPP201100603)
URE's Mitigation Plan to address its violation of CIP-007-1 R6.5 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 SPPMIT006637 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to create and implement a procedure to ensure that the review of the Oracle Listener logs is properly documented.

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-004-3 R2.1; R3; R4.1 and R4.2 (SPP2012009554, SPP2012009984, and SPP2012009762)
URE's Mitigation Plan to address its violation of CIP-004-3 R2.1 (SPP2012009554) 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 SPPMIT007947-1 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 (SPP2012009984) 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 SPPMIT007949-1 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 R4.1 and R4.2 (SPP2012009762) 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 SPPMIT007948-1 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 SPPMIT007947-1 requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

URE certified that the above Mitigation Plan SPPMIT007949-1 requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plans for SPP2012009554 and SPP2012009984 were completed.

URE certified that the above Mitigation Plan SPPMIT007948-1 requirements were completed. URE submitted evidence of completion of its Mitigation Plans.

After reviewing URE's submitted evidence, SPP RE verified that URE's Mitigation Plan for SPP2012009762 were completed.

CIP-007-3 R5.1.1 (SPP2012010535)

URE's Mitigation Plan to address its violation of CIP-007-3 R5.1.1 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 SPPMIT007950-1 and was submitted as non-public information to FERC in accordance with FERC orders.

URE's Mitigation Plan required URE to:

1. Modify its system engineering user management procedure to ensure the procedure was in line with company policies, company processes, and NERC Reliability Standards; and
2. Train its system engineering staff on the updated Procedure.

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

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

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[9]

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,[10] 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 seven thousand dollar ($107,000) financial penalty against URE and other actions to facilitate future compliance required under the terms and conditions of the Settlement Agreement. In approving the Settlement Agreement, the NERC BOTCC reviewed the applicable requirements of the Commission-approved Reliability Standards and the underlying facts and circumstances of the violations at issue.

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

1. URE's Internal Compliance Program (ICP);

[9] *See* 18 C.F.R. § 39.7(d)(4).
[10] *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).

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, as described above;
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 seven thousand dollars ($107,000) 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, SPP201000421, included as Attachment B to the Settlement Agreement;
3. SPP RE's Disposition of Violation for CIP-007-3 R9, SPP201100526, included as Attachment C to the Settlement Agreement;
4. SPP RE's Disposition of Violation for CIP-003-3 R6, SPP201100535, included as Attachment D to the Settlement Agreement;
5. SPP RE's Disposition of Violation for CIP-007-3 R1.1, SPP201100536, included as Attachment E to the Settlement Agreement;
6. SPP RE's Disposition of Violation for CIP-004-3 R4.2, SPP201100557, included as Attachment F to the Settlement Agreement;
7. SPP RE's Disposition of Violation for CIP-005-1 R1, SPP201100558, included as Attachment G to the Settlement Agreement;
8. SPP RE's Disposition of Violation for CIP-002-1 R2, SPP201100596, included as Attachment H to the Settlement Agreement;
9. SPP RE's Disposition of Violation for CIP-005-1 R4.2, SPP201100598, included as Attachment I to the Settlement Agreement;
10. SPP RE's Disposition of Violation for CIP-006-1 R1.1 and R1.8, SPP201100600, included as Attachment J to the Settlement Agreement;
11. SPP RE's Disposition of Violation for CIP-007-1 R3.2, SPP201000601, included as Attachment K to the Settlement Agreement;
12. SPP RE's Disposition of Violation for CIP-007-1 R5.1.1, R5.2, R5.2.3, R5.3.3, SPP201100602, 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, SPP2012009554, SPP2012009984 and SPP2012009762, included as Attachment M to the Settlement Agreement;
14. SPP RE's Disposition of Violation for CIP-007-3 R5.1.1, SPP2012010535, included as Attachment N to the Settlement Agreement;

b) Record documents for the violations of CIP-003-1 R5.2, SPP201000421, included as Attachment b:

1. URE's Self-Report for SPP201000421;
2. URE's Mitigation Plan for SPP201000421 designated as SPPMIT005058;
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-007-3 R9, SPP201100526, included as Attachment c:

1. URE's Self-Report for SPP201100526;
2. URE's Mitigation Plan for SPP201100526 designated as SPPMIT005069;
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-003-3 R6, SPP201100535, included as Attachment d:

1. URE's Self-Report for SPP201100535;
2. URE's Self-Report for SPP201100535;
3. URE's Self-Report for SPP201100535;
4. URE's Mitigation Plan for SPP201100535 designated as SPPMIT007952-1;
5. URE's Certification of Mitigation Plan Completion; and
6. SPP RE's Verification of Mitigation Plan Completion.

e) Record documents for the violations of CIP-007-3 R1.1, SPP201100536, included as Attachment e:

1. URE's Self-Report for SPP201100536;
2. URE's Mitigation Plan for SPP201100536 designated as SPPMIT007946-1;
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 R4.2, SPP201100557, included as Attachment f:

1. URE's Self-Report for SPP201100557;
2. URE's Mitigation Plan for SPP201100557 designated as SPPMIT006556;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

g) Record documents for the violations of CIP-005-1 R1, SPP201100558, included as Attachment g:

1. URE's Self-Report for SPP201100558;
2. URE's Mitigation Plan for SPP201100558 designated as SPPMIT006608;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

h) Record documents for the violations of CIP-002-1 R2, SPP201100596, included as Attachment h:

1. SPP RE's Source document for SPP201100596;
2. URE's Mitigation Plan for SPP201100596 designated as SPPMIT006652;
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, SPP201100598, included as Attachment b:

1. SPP RE's Source document for SPP201100598 (see Attachment h-1);
2. URE's Mitigation Plan for SPP201100598 designated as SPPMIT006607;
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, SPP201100600, included as Attachment b:

1. URE's Self-Report for SPP201100600;
2. URE's Self-Report for SPP201100600;
3. SPP RE's Source document for SPP201100600 (see Attachment h-1);
4. URE's Mitigation Plan for SPP201100600 designated as SPPMIT006634;

5. URE's Certification of Mitigation Plan Completion ; and
6. SPP RE's Verification of Mitigation Plan Completion.

k) Record documents for the violations of CIP-007-1 R3.2, SPP201000601, included as Attachment b:

1. URE's Self-Report for SPP201000601;
2. URE's Self-Report for SPP201000601;
3. SPP RE's Source document for SPP201000601 (see Attachment h-1);
4. URE's Mitigation Plan for SPP201000601 designated as SPPMIT005058;
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 R5.1.1, R5.2, R5.2.3, R5.3.3, SPP201100602, included as Attachment b:

1. URE's Self-Report for SPP201100602;
2. SPP RE's Source document for SPP201100602 (see Attachment h-1);
3. URE's Mitigation Plan for SPP201100602 designated as SPPMIT006636;
4. URE's Certification of Mitigation Plan Completion; and
5. SPP RE's Verification of Mitigation Plan Completion.

m) Record documents for the violations of CIP-007-1 R6.5, SPP201100603, included as Attachment b:

1. SPP RE's Source document for SPP201100603 (see Attachment h-1);
2. URE's Mitigation Plan for SPP201100603 designated as SPPMIT006637;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

n) Record documents for the violations of CIP-004-3 R2.1, R3, R4.1 and R4.2, SPP2012009554, SPP2012009984 and SPP2012009762, included as Attachment b:

1. URE's Self-Report for SPP2012009554;
2. URE's Self-Report for SPP2012009984;
3. URE's Self-Report for SPP2012009762;

4. URE's Self-Report for SPP2012009762;
5. URE's Mitigation Plan for SPP2012009554 designated as SPPMIT007947-1;
6. URE's Mitigation Plan for SPP2012009984 designated as SPPMIT007949-1;
7. URE's Mitigation Plan for SPP2012009762 designated as SPPMIT007948-1;
8. URE's Certification of Mitigation Plan Completion for SPP2012009554;
9. URE's Certification of Mitigation Plan Completion for SPP2012009984;
10. SPP RE's Verification of Mitigation Plan Completion for SPP2012009554 and SPP2012009984;
11. URE's Certification of Mitigation Plan Completion for SPP2012009762; and
12. SPP RE's Verification of Mitigation Plan Completion for SPP2012009762.

o) Record documents for the violations of CIP-007-3 R5.1.1, SPP2012010535, included as Attachment o:

1. URE's Self-Report for SPP2012010535;
2. URE's Mitigation Plan for SPP2012010535 designated as SPPMIT007950-1;
3. URE's Certification of Mitigation Plan Completion; and
4. SPP RE's Verification of Mitigation Plan Completion.

A Form of Notice Suitable for Publication[11]

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

[11] *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