NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

October 30, 2014

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-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 Southwest Power Pool Regional Entity (SPP RE) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SPP RE's determination and findings of the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of forty-five thousand dollars ($45,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and

[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 (2014). *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) and 18 C.F.R § 39.7(d).

[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.

3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
404-446-2560 | www.nerc.com

conditions of the Settlement Agreement. The violations in this Notice of Penalty 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, 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 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SPP2013011798	CIP-005-1	R1	Medium/Severe	$45,000
SPP2013011799	CIP-005-1	R2	Medium/Severe	
SPP2013011800	CIP-005-1	R3	Medium/Severe	
SPP2013011801	CIP-005-1	R4	Medium/Severe	
SPP2013011802	CIP-006-1	R1	Medium/Severe	
SPP2013011804	CIP-007-1	R1	Medium/Severe	
SPP2013011805	CIP-007-1	R2	Medium/Severe	
SPP2013011806	CIP-007-1	R3	Lower/Severe	
SPP2013011807	CIP-007-1	R5	Lower/Severe	
SPP2013011808	CIP-009-1	R1	Medium/Severe	
SPP2013011809	CIP-007-3	R8	Medium/Severe	

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SPP2013012355	CIP-006-1	R1	Medium/Severe	$45,000
SPP2013012356	CIP-004-3	R4	Lower/High	
SPP2013012533	CIP-006-2a	R6	Lower/Severe	
SPP2013012752	CIP-006-2	R3	Medium/Severe	
SPP2013012841	CIP-003-1	R6	Lower/Severe	
SPP2013012842	CIP-004-1	R4	Lower/Moderate	
SPP2013012844	CIP-005-3a	R5	Lower/Lower	
SPP2013012845	CIP-006-2	R1	Medium/Severe	
SPP2013013117	CIP-006-3c	R5	Medium/Severe	

*Violation Risk Factor (VRF) and Violation Severity Level (VSL)

CIP-005-1 R1 (R1.5) (SPP2013011798)

URE submitted a Self-Report stating that it did not correctly identify four devices as electronic access points to its electronic security perimeters (ESPs). Later, URE supplemented its Self-Report, explaining that it also failed to identify two receiver devices as access points to the ESP. During its review, SPP RE further determined that URE had not subjected the identified access points to the controls identified in CIP-005-1 R1.5 where technically feasible. Additionally, the access points were not afforded some of the required controls due to technical infeasibility, but they did not have a technical feasibility exception (TFE). In its original Self-Report, URE also indicated it did not afford a number of the protective measures required by CIP-005-1 R1.5 to its two servers residing outside the ESP.

SPP RE determined that URE had a violation of CIP-005-1 R1.5 for failing to identify certain devices as electronic access points to the ESPs, and for failing to afford a number of required controls and protective measures to these devices.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the bulk power system (BPS), but did not pose a serious or substantial risk. Specifically, with respect to the two servers, a failure to adequately secure the servers makes access credentials vulnerable to potential theft by malicious actors. Stolen access credentials could be used to gain access to the ESP, and thereby compromise network assets used to support the reliable operation of the BPS. Nevertheless, URE had instituted a number of controls to guard against unauthorized access to the servers, including housing the servers within a physical access controlled corporate data center, and limiting electronic access to the servers to information technology (IT) system administrators.

Regarding the four devices, the failure to apply appropriate controls increased the risk that a malicious actor might successfully access URE's ESP. SPP RE determined that the role and position of the devices in the URE network limited the risk posed by the inability of the devices to implement the identified technical controls. Further, each of the devices resides within a physical security perimeter (PSP).

URE's Mitigation Plan to address this violation was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. remove the servers from their role in ESP; and
2. document the devices and file TFEs.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R2 (R2.1; R2.2; R2.4; and R2.5) (SPP2013011799)

URE submitted a Self-Report stating that it failed to request TFEs for two switches and two additional devices. Additionally, URE's energy management system (EMS) vendor was not required to authenticate itself as an accessing party at the URE ESP firewalls. Later, URE supplemented its Self-Report, stating that it also failed to request a TFE for two devices that were not capable of authenticating the accessing party, and did not subject these devices to the documentation requirements of R2.5.

During a Compliance Audit (Compliance Audit), SPP RE discovered that URE placed a jump box4 into service to facilitate interactive access into the ESP, but failed to ensure the authenticity of the accessing parties when the jump box was accessed through a utility server.

SPP RE determined that URE had a violation of CIP-005-1 R2.1, R2.2, R2.4, and R2.5 for failing to: i) request TFEs for several devices; ii) require a vendor to authenticate itself; and iii) authenticate the accessing parties to the jump box.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The vendor was required to authenticate at the URE corporate firewall before crossing the ESP firewall, and the final grant of vendor access required affirmative action by URE to allow access at the corporate firewall. URE never granted the vendor access via its corporate firewall.

The role and position of the devices at issue in the URE network limited the risk posed by the inability of the devices to implement the identified technical controls. Additionally, some of the devices at issue resided within a PSP.

Although any of the eight unauthorized employees with access to the utility server could have attempted to access the jump box, access would have been denied for lack of credentials, i.e., an approved username and password combination. Furthermore, URE continuously monitored its network with a network monitoring utility that is set to alert for unauthorized changes in network device configurations.

URE's Mitigation Plan to address this violation was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. document the devices at issue as access points;
2. request TFEs as needed;
3. establish and implement a foot patrol inspection procedure;
4. confirm that remote desktop protocol for interactive access to the ESP access point follows an encrypted connection; and

[4] A jump box is a secured computer that administrators log onto in order to gain access to other computers and administer them. The jump box is designed to provide an extra layer of security.

5. remove the utility server with multiple user accounts from being able to access the jump host.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R3 (R3.1 and R3.2) (SPP2013011800)
URE submitted a Self-Report stating that four of its electronic access points were not capable of monitoring, logging, or alerting for electronic access attempts into URE's ESP. Although access attempts to the switches were logged and monitored during electronic sessions via URE's security monitoring, analysis, and response system, no logging was occurring when IT personnel physically connected at the switches for administrative purposes. Later, URE supplemented its Self-Report, explaining that it also did not identify two devices that were not capable of monitoring, logging, or alerting for electronic access attempts at those devices.

SPP RE determined that URE had a violation of CIP-005-1 R3.1 and R3.2 for failing to monitor electronic access to four electronic access points and two devices.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The switches reside within URE's PSP and physical access to the switches would require access to the PSP. Furthermore, the EMS was receiving information related to logging and alerts. Finally, URE continuously monitors and alerts for malicious activity on its network.

URE's Mitigation Plan was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. remove switches as access points;
2. document the devices at issue as access points;
3. request a TFE as needed; and
4. establish and implement a foot patrol inspection procedure.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-1 R4 (R4.2, R4.3, R4.4, and R4.5) (SPP2013011801)

URE submitted a Self-Report stating that it did not implement a cyber-vulnerability assessment (CVA) process that included: i) a review to verify that only ports and services required for operations at access points were enabled; ii) the discovery of all access points to the ESP; iii) a review of controls for default accounts, passwords, and network management community strings; and iv) documentation of the results of the assessment.

URE's CVA procedure only partially satisfied the requirements of R4.3. Additionally, URE did conduct ports and services verifications during the annual review of its access point configurations.

SPP RE determined that URE had a violation of CIP-005-1 R4.2 to R4.5 for failing to perform a CVA as required by this Standard.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of a documented action plan for assessing CVA-identified vulnerabilities increased the risk that URE might fail to address vulnerabilities impacting its EMS. Additionally, failure to evaluate all access points increased the risk of potential malicious access to the URE ESP. However, URE was running scans from inside its ESP to identify all connected devices within the network, scanning active ports and services on devices, and scanning devices for vulnerabilities on an ongoing basis. During the pendency of the violation, URE was verifying the operational necessity of its enabled ports and services during its annual review of its access point configurations. Finally, URE conducted monitoring of network device hardware status, configuration, and behavior at all times.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to conduct a CVA and ensure that:

1. all ports and services were identified;
2. all access points were identified;
3. a review of controls for default accounts, passwords, and network management community strings was conducted; and
4. the assessments results were adequately documented.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R1 (R1.8) (SPP2013011802)
URE submitted a Self-Report stating that its system controllers are incapable of providing a number of the protective measures controls included in CIP-007, and TFEs were not requested. Specifically, URE did not: i) enable only the ports and services required for normal operations; ii) implement security patch management; iii) implement malicious software prevention; iv) implement the required password complexity; or v) implement security status monitoring.

SPP RE determined that URE had a violation of CIP-006-1 R1.8 for failing to provide the protective controls listed above.

SPP RE determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE through when SPP RE accepted URE's TFEs.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE afforded the controllers all of the protective measures specified in R1.8 that were technically feasible. Although it could not apply the measures to the controls identified in the violation, it did apply those controls to the server that manages the controllers.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to request a TFE for the controllers at issue.

CIP-007-1 R1 (R1.1, R1.2, and R1.3) (SPP2013011804)
URE submitted a Self-Report stating that: i) it did not have test procedures for third-party software; ii) it did not ensure that third-party patches which were applied did not adversely affect existing cybersecurity controls; and iii) it did not document test results for testing conducted on some of its Cyber Assets as required by R1.3.

During the Compliance Audit, SPP RE determined that URE's cybersecurity testing procedures did not require testing of software upgrades for a third-party proprietary network monitoring device located within the ESP.

SPP RE determined that URE had a violation of CIP-007-1 R1.1 to R1.3 for failing to: i) have test procedures for some devices; ii) ensure all patches would not adversely affect the controls, and iii) document the test result for some of its Cyber Assets.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement a testing process for third-party patches presented a risk that patches might be installed in the production environment prior to vetting and could adversely affect the existing cybersecurity controls. Additionally, a failure to maintain patch records decreased URE's ability to conduct after- the-fact event analysis should a patch have an adverse effect on URE's network and ensure that testing was being conducted in accordance with procedural requirements. However, URE deployed all patches in its stand-by environment initially, scanned the host and network devices in that environment, and only after identifying that no adverse effects existed did URE deploy the patches to the operational environment. This process was consistent with URE's patch management procedure.

URE's failure to test software upgrades to the network monitoring device created a risk that the implementation of the upgrades could adversely affect the security controls configured on the device, thereby making it susceptible to malicious attack. However, URE runs a vulnerability scanning utility on a daily basis to monitor for configuration changes to devices in its environment. Additionally, the network monitoring device limited the impact of this violation.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. identify all EMS hardware that is regulated by the CIP standards;
2. develop a list of all applications residing on that hardware;
3. develop a list of databases residing on that hardware;
4. identify a reliable source for security patch update information for the assets identified;
5. develop a security patch tracking mechanism;
6. develop a process to assess identified patches;
7. develop a timeline to test and implement identified patches;

8. develop a process to address applicable patches that cannot be installed due to operational impact;
9. develop a process to ensure that all patch implementations are appropriately documented; and
10. modify its change control and configuration management process to ensure the appropriate testing of proprietary systems.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R2 (R2.1 and R2.2) (SPP2013011805)
URE submitted a Self-Report stating that, although URE was aware of enabled ports and services, it had not maintained a documented baseline of those ports and services that were required for normal or emergency operations.

SPP RE determined that URE had a violation of CIP-007-1 R2.1 and R2.2 for failing to determine that only required ports and services were enabled.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, a failure to document those ports and services required for normal and emergency operations created a risk that URE would fail to disable unneeded ports and services on hosts residing within its ESP. The failure to disable such ports or services increased the attack surface available to a potential malicious actor and weakened URE's ability to identify unauthorized changes that may have occurred in the environment. Nevertheless, URE had maintained an operational awareness of the port and service changes. Additionally, the devices at issue resided behind hardened firewalls, and were guarded by updated anti-malware software.

URE's Mitigation Plan was submitted to SPP RE.

URE's Mitigation Plan required URE to:

1. create a baseline for those ports and services that were required for normal or emergency operations; and

2. review the ports and services on that baseline to ensure only the ports and services required for normal and emergency operations were enabled.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R3 (R3.1 and R3.2) (SPP2013011806)

URE submitted a Self-Report stating that it did not document a security patch management program for tracking, evaluating, testing, and installing third-party cybersecurity software patches for Cyber Assets within the ESP. Moreover, URE's patch management program did not address the assessment and installation of third-party patches. Furthermore, four patches were not assessed within 30 days of release.

SPP RE determined that URE had a violation of CIP-007-1 R3.1 and R3.2 for failing to document a patch management program for certain patches and failing to assess four patches in a timely fashion.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, the lack of a documented and formalized process for patch management creates a risk that an ad hoc approach may be relied on for patch management. Such an approach might result in missed patches or patch implementations that have not been fully vetted and that pose a risk to existing cybersecurity controls inside URE's ESP. Nevertheless, URE did demonstrate an operational awareness of its third-party patch management process. SPP RE's review determined that while the patches were operationally important, they were not patches deployed to mitigate vulnerabilities on the host operating systems.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop and implement a procedure for the tracking and evaluation of third-party security patches; and
2. assess the missed patches.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-1 R5 (R5.1.2; R5.1.3; R5.2.3 and R5.3.2) (SPP2013011807)
URE submitted a Self-Report stating that URE did not: i) implement an audit trail for shared account use; ii) log successful individual local and domain user access attempts; and iii) enforce the required password complexity for certain accounts.

Additionally, during the Compliance Audit, SPP RE discovered an additional violation of CIP-007-1. Specifically, URE did not provide evidence that: i) the use of one shared account discovered during a CVA was reviewed or that specific users of the account were identified; ii) it reviewed access privileges for local accounts on the physical security server; iii) it maintained an audit trail of account use for the shared account discovered during the CVA; and iv) it subjected one router's user level password to the password complexity requirements.

SPP RE determined that URE had a violation of CIP-007-1 R5.1.2; R5.1.3; R5.2.3; and R5.3.2 for failing to maintain and provide evidence of its actions taken pursuant to these subrequirements.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, URE's failure to implement all the required CIP account controls diminished URE's ability to maintain an awareness of and accountability for the use of accounts and associated privileges, which could hinder URE's ability to respond to the misuse of accounts in its environment. Additionally, the failure to establish passwords meeting the complexity requirements creates a risk that the accounts could be more susceptible to brute force password attacks. However, URE grants access on a need-to-know basis, which bolsters its ability to maintain an operational awareness of changes occurring in its environment. The CVA-identified account was not normally used by URE, and its use would have been limited to three individuals.

Regarding the physical security server, the accounts URE failed to review were limited to five individuals.

Regarding URE's inability to technically enforce the required password complexity for certain accounts, URE did procedurally require the use of a password generator to establish passwords meeting the complexity requirements.

Regarding local and domain user logging, URE was logging unsuccessful account attempts and was also logging inter-system login attempts, both successful and unsuccessful.

All account access was limited to individuals who had undergone personnel risk assessments (PRA) and CIP training. Additionally, URE utilized a network scanning utility and a vulnerability scanning utility on a daily basis to detect unauthorized configuration changes on ESP network and host machines.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. implement paper-based manual logging where shared administration accounts are being used;
2. request a TFE for the inability of some applications to enforce the password complexity requirements;
3. remove the CVA-identified shared account;
4. establish detailed records of physical security server account reviews;
5. begin maintaining logs of successful local and domain account logins; and
6. change the password on the router at issue to meet the password complexity requirements.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-009-1 R1 (R1.1 and R1.2) (SPP2013011808)
URE submitted a Self-Report stating that it had not created a recovery plan for several of its physical system components.

During the Compliance Audit, SPP RE discovered an additional violation of CIP-009-1 R1.1 and R1.2. Specifically, an URE electronic access control and monitoring (EACM) device failed when its hardware was replaced. Although the EACM device was restored to its original state, URE's recovery plan did not specify the required actions to respond to events or conditions of varying duration and severity or the defined roles and responsibilities of responders for the EACM device.

SPP RE determined that URE had a violation of CIP-009-1 R1.1 and R1.2 for failing to have a recovery plan for some of its components, and for failing to specify in its recovery plan the actions necessary to recover from a failure of its EACM device.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE physical system components were designed to default to secure mode. Also, the EACM device was restored after the system failure, and URE implemented manual log review in the interim.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. create a recovery plan for the physical system components ; and
2. create a recovery plan for the EACM device.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-007-3 R8 (R8.2; R8.3 and R8.4) (SPP2013011809)
URE submitted a Self-Report stating that URE did not conduct a review of controls for default accounts and did not document an action plan as part of its annual CVA.

Additionally, during the Compliance Audit, SPP RE discovered an additional violation for CVAs occurring prior to the self-reported instance of noncompliance. URE's CVAs for three consecutive years each shared several deficiencies.

SPP RE determined that URE had a violation of CIP-007-3 R8.2; R8.3; and R8.4 for failing to conduct CVAs that met these subrequirements.

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

SPP RE determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. The lack of a documented action plan for assessing CVA-identified vulnerabilities increases the risk that URE might fail to address vulnerabilities impacting the EMS that could be maliciously exploited to the detriment of BPS operations. However, URE ran both a network scanner and vulnerability scanner that provided URE with an ongoing operational awareness of the ports and services and accounts enabled in its environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. to perform a CVA; and

2. verify that the CVA performed includes all required elements.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-1 R1 (R1.1 and R1.3) (SPP2013012355)
URE submitted a Self-Report stating that it had designated two centers as one ESP. However, the centers did not share one PSP and were connected by a fiber optic circuit. Because a completely enclosed border could not be provided for the fiber circuit, URE was required to implement an alternative physical control measure, but did not do so.

Additionally, URE has a set of double-doors that had not been considered as an access point to a PSP, and therefore had not been subjected to the processes, tools, and procedures for monitoring physical access to the PSP.

SPP RE determined that URE had a violation of CIP-006-1 R1.1 and R1.3 for failing to provide an alternative physical control measure for the fiber circuit at issue, and failing to consider a door as being an access point to its PSP.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The fiber circuit is owned by and within the sole control of URE. The double-doors at issue were only utilized for the moving of large equipment. Additionally, the facility was manned at all times, and the doors were subject to video monitoring, thereby heightening URE's awareness of any intrusion in the environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. alarm the double doors and institute monitoring by personnel; and

2. implement a procedure, which outlined a response plan for loss of fiber continuity.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-004-3 R4 (R4.2) (SPP2013012356)
URE submitted a Self-Report stating that it failed to revoke an employee's physical access to CCAs within seven days of that employee no longer requiring access.

SPP RE determined that URE had a violation of CIP-004-3 R4.2 for failing to revoke one employee's physical access to CCAs in a timely fashion.

SPP RE determined the duration of the violation to be from the date the employee's physical access should have been revoked, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The employee was an URE employee, remained employed by URE through the violation period, and had undergone appropriate training regarding the treatment of CCAs. Lastly, the employee could only have entered the relevant PSP using his employee badge, which would have recorded his entry into the environment.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to revoke the employee's physical access to the CIP areas.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2a R6 (SPP2013012533)
URE submitted a Self-Report to SPP RE stating that it had placed an emergency access badge in a lower security environment to enable access from outside the PSP in the event of a medical emergency. In the event the badge were used, the associated log did not provide sufficient information to uniquely identify individuals and the time of access.

SPP RE determined that URE had a violation of CIP-006-3c R6 for failing to ensure that the log for the security badge at issue identified all individuals and the time of their access.

SPP RE determined the duration of the violation to be from the date the emergency badge at issue was activated, through when URE completed its Mitigation Plan.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The badge was located inside a facility that required corporate badge access to enter. Furthermore, use of the badge would create a log entry in URE's physical log files, thereby providing an audit trail of badge use.

URE's Mitigation Plan was submitted to SPP RE stating that it had been completed.

URE's Mitigation Plan required URE to deactivate the emergency badge.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2 R3 (SPP2013012752)

URE submitted a Self-Report to SPP RE stating it did not place two Cyber Assets used in the access control and/or monitoring of its ESP within an identified PSP.

SPP RE determined that URE had a violation of CIP-006-2 R3 for failing to place two Cyber Assets within an identified PSP.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had instituted controls to guard against unauthorized access to the Cyber Assets. The Cyber Assets resided within a physical access-controlled corporate data center; electronic access to the Cyber Assets was limited to IT system administrators. Also, the Cyber Assets were subject to the corporate policy for change management and resided behind a corporate firewall.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to remove the Cyber Assets.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-003-1 R6 (SPP2013012841)
During the Compliance Audit, SPP RE determined that URE's change control and configuration management process did not address the replacement and removal of CCA hardware. Additionally, URE did not have a documented process to address disposal of a failed third-party proprietary network monitoring device, nor could it demonstrate that a replacement for the failed device was appropriately implemented.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had evidence to demonstrate that wiping of the failed third-party device had occurred during disposal, and that no harm to its network operations occurred as a result of implementation of the replacement device. Prior to the installation of the new device, the failed device was successfully run on the network for multiple years without any degradation of network operations.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to expand its change control and configuration management process to include third-party proprietary devices.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-004-1 R4 (R4.1) (SPP2013012842)
During the Compliance Audit, SPP RE determined that URE maintained lists of personnel with authorized cyber and unescorted physical access to CCAs. However, URE's quarterly reviews did not include a review of the specific authorized cyber access rights of personnel, as required by this Standard.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Although URE did not review the specific access rights on a quarterly basis, it did: i) maintain an access list with specific access rights; ii) review and modify (if necessary) access rights each time the status of an individual on the access list changed; and iii) grant access to URE's CCAs to

only personnel with cybersecurity training and a PRA. URE also conducted quarterly reviews of its access list, which included re-verification of each individual's status, verification of completion of the required annual cybersecurity training, and determination of the status of each individual's PRA. During mitigation, URE confirmed that each affected employee's specific assigned access rights were correct.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to include in its quarterly reviews of access lists specific authorized cyber access rights of URE personnel.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-005-3a R5 (R5.1 and R5.2) (SPP2013012844)
During the Compliance Audit, SPP RE determined that URE placed a jump box into service. However, URE did not update its documentation to reflect the processes and configurations associated with the device. Additionally, URE removed a virtual private network (VPN) utilized for vendor emergency support, but did not update its ESP network diagram documentation within 90 calendar days of the change.

SPP RE determined that URE had a violation of CIP-005-3a R5.1 and R5.2 for failing to update its documentation related to the jump box, as required, and failing to update its ESP network diagram within 90 days.

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

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE only allows remote access via one jump box device, and the administration of the access model involves a small number of staff. The VPN removal issue was documentation-related.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. update its network diagram documentation to reflect the removal of the VPN;

2. retrain affected staff on timely updating network or controls documentation; and

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-2 R1 (R1.6) (SPP2013012845)
During the Compliance Audit, SPP RE determined that URE did not consistently follow the visitor control program defined in its physical security plan. URE's manual logs for visitor access into its primary and backup control centers contained multiple instances of illegible personnel escort and visitor names, missing and incomplete information, and information listed in the wrong columns.

SPP RE determined the duration of the violation to be from the date of the first identified log deficiency, through the date of the last identified log deficiency.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. As required by URE's procedure, the visitors at issue were all escorted while inside URE's PSP. Furthermore, video monitoring is enabled at URE's facility. Moreover, URE deploys network monitoring to monitor the up/down state of devices within its environment, thereby enabling early detection of attempted sabotage. Lastly, the discrepancies in the visitor logs were the result of inconsistent recording and did not represent complete failures to identify the entering parties.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. develop an example of how the manual log should be filled out; and
2. train personnel on how to properly fill out the manual log.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

CIP-006-3c R5 (SPP2013013117)
URE submitted a Self-Report stating that, following a port scan conducted during URE's 2013 CVA, remote terminal unit (RTU) supporting alarms for URE's PSP door monitoring at its back-up facilities ceased to function. URE detected the failure and brought the alarm functions back on-line.

URE supplemented its Self-Report stating that a technician moved a server, which caused a cable to become disconnected from the aforementioned RTU, again resulting in a loss of alarm functionality. The issue was discovered and fixed.

SPP RE determined that URE had a violation of CIP-006-3c R5 for failing to maintain alarm functionality for an access point to the PSP on two instances.

SPP RE determined the duration of the violation to be from the date of the initial RTU alarm failure, through when the RTU alarm functionality was restored following the second failure.

SPP RE determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The facilities' physical access points are monitored at all times via closed circuit television, and the access systems continued to authorize access appropriately. Notwithstanding the RTU alarm function failure, the RTU continued to log access, and URE determined that no unauthorized access occurred during the time the alarm function was unavailable.

URE's Mitigation Plan was submitted to SPP RE stating it had been completed.

URE's Mitigation Plan required URE to:

1. reboot the RTU to re-establish alarm functionality following the initial failure;
2. reattach the disconnect cable following the second failure; and
3. implement an alarm to notify personnel when the RTU alarm functionality is down.

URE certified that the above Mitigation Plan requirements were completed.

SPP RE verified that URE's Mitigation Plan was complete.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of forty-five thousand dollars ($45,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. URE had prior violations of CIP-003, CIP-004, CIP-005, CIP-006, CIP-007, and CIP-009. SPP RE considered some of these prior violations as aggravating factors in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SPP RE considered a neutral factor;

3. URE agreed to: i) restructure its CIP compliance program; ii) hire an additional system administrator; iii) convene a one-day compliance workshop with SPP RE staff; and iv) enhance its EMS to include an asset management system.
4. URE received mitigating credit for self-reporting the following violations: SPP2013012355, SPP2013012356, and SPP2013013117;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations posed minimal or moderate but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above; and
8. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SPP RE determined that, in this instance, the penalty amount of forty-five thousand dollars ($45,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Statement Describing the Assessed Penalty, Sanction or Enforcement Action Imposed[5]

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,[6] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on October 1, 2014 and approved 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of forty-five thousand dollars ($45,000) is appropriate for the violations and circumstances at issue, and is consistent with NERC's goal to promote and ensure reliability of the BPS.

[5] *See* 18 C.F.R. § 39.7(d)(4).

[6] *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).

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.

Attachments to be Included as Part of this Notice of Penalty

REMOVED FROM THIS PUBLIC VERSION

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

Conclusion

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

Respectfully submitted,

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

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

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

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity

Attachments