July 31, 2017

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. NP17-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding noncompliance by an Unidentified Registered Entity (URE) 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]

NERC is filing this Notice of Penalty, with information and details regarding the nature and resolution of the violations,[3] 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 violations of NERC Critical Infrastructure Protection (CIP) Reliability Standards.

---

[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 (2017). *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.

According to the Settlement Agreement, URE admits to the violations, and has agreed to the assessed penalty of two hundred fifty thousand dollars ($250,000), 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.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement, by and between SPP RE and URE. 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 (2017), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement and herein.

*SR = Self-Report / SC = Self-Certification / CA = Compliance Audit / SPC = Spot Check / CI = Compliance Investigation

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SPP2014014499	CIP-003-3	R2: R2.2	Medium/ Severe	CA	Minimal	$250,000
SPP2014014500	CIP-003-3	R6	Lower/ Severe		Moderate	
SPP2014014513	CIP-004-3a	R4	Lower/ Moderate			
SPP2014014514	CIP-005-3a	R1: R1.5; R1.6	Medium/ Severe			
SPP2014014501	CIP-006-3c	R1: R1.6.1	Medium/ Severe			
SPP2014014502	CIP-006-3c	R2: R2.2	Medium/ Severe			

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SPP2014014505	CIP-007-3a	R1: R1.1	Lower/ Severe	CA	Moderate	$250,000
SPP2014014506	CIP-007-3a	R2: R2.1; R2.2	Medium/ Severe			
SPP2014014507	CIP-007-3a	R4: R4.1	Medium/ Severe			
SPP2014014508	CIP-007-3a	R5: R5.2; R5.2.2	Lower/ Severe			
SPP2015015324	CIP-007-3a	R6: R6.1; R6.4; R6.5	Medium/ Severe			
SPP2014014510	CIP-008-3	R1: R1.6	Lower/ High			
SPP2014014511	CIP-009-3	R2	Lower/ Severe			

SPP2014014499 CIP-003-3 R2: R2.2 - OVERVIEW

SPP RE determined that URE, on multiple occasions, did not document, within 30 calendar days of the effective date, changes to the senior manager assignment with overall responsibility and authority for leading and managing its implementation of, and adherence to, Standards CIP-002-3 through CIP-009-3.

SPP RE determined that this violation posed a minimal and not a serious or substantial risk to the reliability of the bulk power system (BPS). URE attested that a CIP senior manager was in place and responsible for implementation of the URE CIP Compliance program and that there were no cyber security incidents during the time of the violation.

SPP RE determined the duration of the violation to be approximately 10 months, from the date URE failed to document the change in assigned senior manager, through when URE completed its leadership delegation document identifying the senior manager.

To mitigate this violation, URE:

1. reviewed the URE cyber security policy and identified improvements to ensure compliance with CIP-003 R2;
2. updated the cyber security policy based upon recommendations from the policy review;
3. documented the assignment of the current CIP senior manager; and
4. developed a new URE leadership document to include responsibilities for implementing the process and designation of the CIP senior manager and delegates.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014500 CIP-003-3 R6 - OVERVIEW

SPP RE determined that URE did not: 1) design documentation controls supportive of the designed change management process; and 2) execute the change management process as documented. Specifically, there were deficiencies in URE's change request form when compared with the documented change management process. Additionally, URE's change request form for several changes were missing information and thus did not adhere to the URE change management process.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE had a change control process in place at the time of the violation. The affected assets were behind a firewall. URE's Critical Cyber Assets (CCAs) require an authorized user name and password combination to gain access. URE personnel with access to CCAs had CIP training and current personnel risk assessments (PRAs). The CCAs subject to this violation resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 40 months, from the completion date of the mitigation for the prior violation of the same standard and requirement, through the date URE implemented its updated CCM program that controls changes to CCAs.

To mitigate this violation, URE:

1. redesigned its change management process;
2. implemented system monitoring software to support its change management process;

3. implemented change management software to support controls for its change management process; and
4. updated change management process documentation.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014513 CIP-004-3a R4 - OVERVIEW

SPP RE determined that URE did not maintain an accurate list of personnel with authorized unescorted physical access to CCAs. URE authorized its Physical Access Control Systems (PACS) vendor to grant some vendors and a URE employee access to URE's Physical Security Perimeters (PSPs). The PACS vendor mistakenly granted access for over 90 URE employees who were authorized for access to specific, but not all, PSPs.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Most of the employees mistakenly granted access to all PSPs did not know they were granted access. There was one unauthorized access to a PSP, which was reported by the offender. URE's CCAs are physically and electronically segregated. The assets subject to this violation reside within a physical access-controlled data center; the area with CCAs is staffed 24/7, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately one month, from the date the vendor mistakenly granted access to its PSPs for over 90 URE employees, through the date URE removed the unauthorized PSP access for all personnel that had mistakenly been granted such access.

To mitigate this violation, URE:

1. revoked access to the PSPs for the employees who were not authorized to have such access;
2. reviewed and revised the asset list for accuracy; and
3. developed an internal procedure to prevent the creation of accounts prior to granting approved access.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014514 CIP-005-3a R1: R1.5; R1.6 - OVERVIEW

SPP RE determined that URE did not maintain documentation of its Electronic Security Perimeters (ESPs). Specifically, URE failed to: 1) identify and document all access points to the ESPs in violation of R1; 2) ensure that Cyber Assets used in the access control and/or monitoring of the ESPs were afforded protective measures as specified in CIP-003-3 R6 in violation of R1.5; and 3) maintain documentation of its ESP(s), all electronic access points to the ESP(s), and the Cyber Assets deployed for the access control and/or monitoring of access points (EACMs) in violation of R1.6. In the first instance, the servers essential to performing strong authentication for remote interactive access to URE's ESPs were not properly identified as EACMS, in violation of R1. In the second instance, URE did not properly perform its documented change management process when applying changes to its EACMS devices, in violation of R1.5. In the third instance, URE had deficient ESP documentation, in violation of R1.6.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. URE's Cyber Assets resided within a physical access-controlled data center and behind a firewall. Access to Cyber Assets within the PSP was limited to only those with authorized physical and/or electronic access rights. The area with CCAs used in real-time operations of the BPS was staffed 24/7. URE had 24-hour closed-circuit television monitoring of the PSP locations, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 32 months, from the date the first change in assets was not reflected in the ESP diagram, through the date URE reviewed the CCA List and ESP diagram and updated the ESP diagram.

To mitigate this violation, URE:

1. disabled remote access to the EACMS Cyber Assets;
2. updated the change management process to include a step for reviewing and reconciling the CCA list and ESP documentation; and
3. reviewed the CCA list and ESP diagram and updated the ESP diagram to resolve any discrepancies.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014501 CIP-006-3c R1: R1.6.1- OVERVIEW

SPP RE determined that URE did not properly document the entry and exit of visitors, including the date and time, to and from its PSP. The Audit Team discovered over 20 instances where visitors' entry and/or exit times were not recorded.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE implemented password complexity and lockout policies to reduce the risk of unauthorized access. All personnel with authorized access to Cyber Assets had CIP training and current PRAs. URE's Cyber Assets resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. A majority of the deficient log entries were for janitorial staff who had completed cyber security training and possessed a valid PRA.

SPP RE determined the duration of the violation to be over 27 months, from the day after completion of the mitigation plan for a previous violation of the same Standard and requirement, through the last recorded instance of a deficient visitor log entry.

To mitigate this violation, URE:

1. began maintaining separate visitor logs for each of the PSPs and the common area of the building;
2. updated the visitor access procedure;
3. trained applicable URE personnel on the new visitor access procedure;
4. added a process for review and validation of visitor logs on a daily and quarterly basis to confirm that visitor log procedures have been followed and to promptly address any issues. Identified issues will be documented and reported via a new policy exception form; and
5. instituted periodic compliance spot checks to validate the proper execution of the visitor access policies and procedures.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014502 CIP-006-3c R2: R2.2- OVERVIEW

SPP RE determined that URE did not provide its PACS the protective measures specified in CIP-003-3 R6, CIP-007-3 R2.1, and CIP-007-3 R2.2 when a change was made to the PACS without appropriate

change control or security controls testing. Cyber Assets that authorize and/or log access to PSP(s), exclusive of hardware at the PSP access point(s), were not afforded the protective measures in CIP-003-3 R6. Specifically, URE failed to implement its change management process when making changes to the PACS workstation server, and change request forms for several changes involving PACS were incomplete and thus did not adhere to URE's change management processes. URE failed to implement its process to ensure only those ports required for normal and emergency operations were enabled as required by CIP-007-3 R2.1 and that all other ports were disabled as required by CIP-007-3 R2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. The PACS resided on a network separate from URE's energy management system, with a firewall separating it from the corporate network. The PACS host server resided within a PSP, requiring local access to manage, add users, or make system changes. All personnel with access to Cyber Assets had CIP training and current PRAs. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 30 months, from the day after completion of the mitigation plan for a previous violation of the same Standard and requirement, through the date URE implemented its updated change management program.

To mitigate this violation, URE:

1. redesigned its change management process;
2. implemented system monitoring software to support its change management process;
3. implemented change management software to include controls for its change management process; and
4. updated change management process documentation.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014505 CIP-007-3a R1: R1.1 - OVERVIEW

SPP RE determined that URE did not implement cyber security test procedures in a manner that minimized adverse effects on the production system or its operation. URE implemented a system version update was implemented without prior installment in a testing environment, as required by URE's cyber security test procedures. Additionally, URE failed to demonstrate that testing had been

performed for a firewall configuration change, a switch configuration change, and a change involving operating system patching, as required by URE's change management procedure.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. The Cyber Assets subject to this violation resided within a physical access-controlled data center and behind a firewall. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be over 32 months, from the completion date of the mitigation plan for a prior violation of the same Standard and requirement, through when URE completed its mitigation.

To mitigate this violation, URE:

1. redesigned, implemented, and documented its change management program to include cyber security controls testing of all significant changes, including vendor changes; and
2. implemented system reports and alerts as detective and preventive controls to support change management.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014506 CIP-007-3a R2: R2.1; R2.2 - OVERVIEW

SPP RE determined that URE did not ensure that only ports and services required for normal and emergency operations were enabled on all Cyber Assets within the ESP. Specifically, URE failed to demonstrate the need for a number of ports and services open on its servers by either documenting them as being necessary, closing them, or obtaining a Technical Feasibility Exception (TFE). URE could not demonstrate that it had enabled only those ports required for normal and emergency operations as required by R2.1. As the enabled ports identified in R2.1 were not included in URE's documented ports baseline, URE was unable to ensure that other ports had been disabled prior to production use of the servers inside the ESP or were covered by a TFE as required by R2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place

at the time of the violation. The Cyber Assets subject to this violation resided within a physical access-controlled data center and behind a firewall. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 17 months, from the date of the cyber vulnerability assessment report that identified the undocumented ports, through the date URE documented and began controlling ports and services required for normal and emergency operations.

To mitigate this violation, URE:

1. requested a TFE for two PACS devices for which it is not technically feasible to configure ports and services;
2. reviewed the baselines to confirm which ports were required;
3. implemented a change management procedure to support review and update of baseline documentation; and
4. implemented software to monitor the ports and notify staff of any system changes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014507 CIP-007-3a R4: R4.1 - OVERVIEW

SPP RE determined that URE did not configure the anti-virus client properly during the installation of anti-virus and malware prevention software on an energy management system console. As a result, the software was unable to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on the console.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. Only one console was involved in the violation. There were also protective measures in place at the time of the violation. The console resided within a physical access-controlled data center and behind a firewall. Where technically feasible, anti-virus and malware prevention tools were implemented on the other Cyber Assets located within URE's ESP. All URE personnel with authorized access to Cyber Assets had CIP training and current PRAs. URE's Cyber Assets resided within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS was

staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 24 months, from the date the console was commissioned without the implementation of anti-virus and malware prevention tools, through the date URE implemented the necessary software.

To mitigate this violation, URE:

1. configured the anti-virus software on the console;
2. updated the daily checklist to include more detailed information related to the status of anti-virus software running on Cyber Assets;
3. implemented software to report on anti-virus signature updates for all in-scope Cyber Assets;
4. configured anti-virus software to send email alerts and daily scan reports; and
5. configured system monitoring software to monitor the status of anti-virus running on all in-scope Cyber Assets capable of running anti-virus.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014508 CIP-007-3a R5: R5.2; R5.2.2 - OVERVIEW

SPP RE determined that URE did not document multiple shared default administrator accounts in URE's master account management list in accordance with URE's account management process per CIP-007-3 R5.2. Additionally, because the multiple shared default administrator accounts had not been documented on URE's master account management list, the individuals with access to such accounts were also not identified on the list per R5.2.2.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE's CCAs require an authorized user name and password combination in order to gain access. All personnel with authorized access to Cyber Assets have CIP training and current PRAs. The Cyber Assets subject to this violation reside within a physical access-controlled data center; the area with CCAs used in real-time operation of the BPS is staffed 24/7, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately five months, from the date shared default administrator accounts and users of such accounts were incorrectly documented, through the date URE updated its checklist to reflect the correct system accounts and users.

To mitigate this violation, URE:

1. corrected the account list to reflect the actual default administrator account names;
2. implemented change management software to support user documentation updates;
3. documented the change management process based on the new software;
4. established a quarterly review of shared user accounts; and
5. implemented system notifications to notify certain staff of changes to user accounts.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2015015324 CIP-007-3a R6: R6.1; R6.4; R6.5 - OVERVIEW

SPP RE determined that URE did not implement technical and procedural mechanisms for monitoring security events on all Cyber Assets within the ESP as required by R6.1. Subsequent to SPP RE's determination, URE identified that it did not retain all logs for 90 calendar days as required by R6.4 or review logs of system events related to cyber security and maintain records documenting review of logs as required by R6.5. In two instances, URE failed to collect security event logs and failed to monitor for security events for approximately four months and one month, respectively. URE rebooted a switch, and all log events for approximately three months that had not been saved from the switch, other than critical warnings, were lost.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE's Cyber Assets reside within a physical access-controlled data center and behind a firewall. Where technically feasible, anti-virus and malware prevention tools are implemented on Cyber Assets located within URE's ESP. Access to Cyber Assets within the ESP is limited to only those individuals with authorized physical and/or electronic access rights. All personnel with authorized access to Cyber Assets have CIP training and current PRAs. The area with CCAs used in real-time operation of the BPS is staffed 24/7. URE has 24-hour closed-circuit television monitoring of the PSP locations, and physical security events are investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 16 months, from the first date certain logs were not monitored for security events, through the last date that a manual review of logs was not performed.

To mitigate this violation, URE:

1. reinstituted a manual log retention and review process;
2. implemented software for automated log collection, retention, alerting, and reporting for all in-scope Cyber Assets; and
3. updated procedures to include the new processes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014510 CIP-008-3 R1: R1.6 - OVERVIEW

SPP RE determined that although URE conducted exercises intended to test its Cyber Security Incident Response Plan (CSIRP), there were multiple years in which the evidence provided did not demonstrate that URE followed the necessary steps required by the URE CSIRP.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. URE did have a documented CSIRP in place. URE's CCAs resided within a physical access-controlled data center and behind a firewall. All personnel with authorized access to CCAs had CIP training and current PRAs. The area with CCAs used in real-time operations of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber security incidents during the violation.

SPP RE determined the duration of the violation to be approximately 24 months, from the date the CSIRP should have been tested, through the date URE performed and documented a full test of its CSIRP.

To mitigate this violation, URE:

1. performed a paper drill test of its CSIRP, including a step-by-step exercise of the CSIRP;
2. documented and distributed a summary of the CSIRP exercise to participants for comments;
3. revised the CSIRP; and

4. hired additional staff to monitor and manage CIP-related policies, procedures, and processes.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

SPP2014014511 CIP-009-3 R2 - OVERVIEW

SPP RE determined that although URE conducted exercises intended to exercise its recovery plan, there were multiple years in which the evidence provided did not demonstrate that the specified response actions required by the recovery plan were followed.

SPP RE determined that this violation posed a moderate and not a serious or substantial risk to the reliability of the BPS. The risk to the reliability of the BPS was mitigated by protective measures in place at the time of the violation. As a corrective control, URE could move operational control to standby assets and backup control centers, which would have allowed URE to remain operational in the event the primary control center was compromised. URE's CCAs were physically and electronically segregated, located behind a firewall, and requiring an authorized user name and password combination in order to gain access. All personnel with access to Cyber Assets had CIP training and current PRAs. The area with CCAs used in real-time operations of the BPS was staffed 24/7, and physical security events were investigated by local security. URE attested that there were no cyber incidents during the violation.

SPP RE determined the duration of the violation to be approximately 40 months, from the date of the deficient recovery plan exercise, through the date URE performed a recovery plan exercise that documented the followed response actions required by the recovery plan.

To mitigate this violation, URE:

1. assigned a CIP senior manager;
2. provided recovery plan training to energy management system personnel;
3. performed and documented an exercise of its recovery plan; and
4. scheduled the next annual recovery plan exercise.

URE certified that it had completed its mitigation activities, and SPP RE verified that URE had completed all mitigation activities.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SPP RE has assessed a penalty of two hundred fifty thousand dollars ($250,000) for the referenced violations. In reaching this determination, SPP RE considered the following factors:

1. SPP RE considered URE's compliance history and determined that URE had one prior violation each of CIP-003 R6; CIP-004 R4; CIP-005 R1; CIP-006-3 R2.2; CIP-006-3c R1.6.1; and CIP-007 R2, R4, R5, and R6. URE had two prior violations each of CIP-007 R1; CIP-008 R1.6; and CIP-009 R2. SPP RE aggravated the penalty for these violations, as they were repeat noncompliance with the subject NERC Reliability Standards;
2. SPP RE considered URE's delay in submitting and implementing its Mitigation Plans an aggravating factor. URE submitted several Mitigation Plans at least 15 months after the Compliance Audit, some of which URE completed over 18 months after the Compliance Audit. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards to improve URE's compliance culture and increase its responsiveness;
3. URE had an internal compliance program (ICP) at the time of the violation, which SPP RE did not consider a mitigating factor because of the number of repeat violations and because URE's ICP did not address the various root causes of the violations. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards, which is designed to improve URE's compliance culture;
4. URE admitted to the violations;
5. URE did not receive cooperation credit because SPP RE experienced difficulty obtaining substantive updates from URE regarding its mitigation progress. URE is hiring additional personnel and engaging with consultants who specialize in compliance with NERC's CIP Reliability Standards to increase its responsiveness and improve its engagements with SPP RE. SPP RE will conduct a Compliance Audit of URE in 2017;
6. URE submitted a Self-Report after receiving a notice of Compliance Audit for one of its instances of noncompliance for SPP2015015324 CIP-007-3 R6.1, R6.4, and R6.5, therefore SPP RE did not apply mitigating credit for the Self-Report;
7. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
8. one violation posed a minimal and not a serious or substantial risk to the reliability of the BPS, and 12 violations posed a moderate risk and not a serious or substantial risk to the reliability of the BPS, as described above;

9. URE agreed to "above and beyond" activities, which SPP RE considered as an offset to the proposed financial penalty. Under the Settlement Agreement, URE will complete the following activities:
    a. URE contracted with a vendor to evaluate its CIP ICP, covering CIP-002 through CIP-011 requirements relating to low and medium impact Bulk Electric System Cyber Systems;
    b. URE will implement substation physical perimeter security;
    c. URE will implement software to analyze firewall and router configurations for the purpose of identifying security vulnerabilities and deviations from URE security policies;
    d. URE contracted with a vendor that performed a targeted Cyber-Vulnerability Assessment (CVA). The vendor will also train URE network security staff on how to use the vulnerability assessment tool for future CVA testing;
    e. URE implemented a program to perform active vulnerability assessments of operating system assets within its ESP on a monthly basis;
    f. A URE employee completed ethical hacker training and received ethical hacker certification, which aids in the use of preventive and detective controls to identify vulnerabilities and exploits specific to checkpoint firewalls;
    g. Certain URE staff will attend industrial control systems cyber security training, which applies the use of preventive and detective controls to identify and respond to vulnerabilities and exploits specific to industrial control systems; and
    h. At least one URE analyst will complete certified ethical hacking training and receive certified ethical hacking certification, which aids in the use of preventive and detective controls to identify and respond to cyber vulnerabilities and exploits.
10. 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 two hundred fifty thousand dollars ($250,000) 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[4]

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,[5] the NERC BOTCC reviewed the Settlement Agreement and supporting documentation on June 15, 2017 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 two hundred fifty thousand dollars ($250,000) 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.

[4] *See* 18 C.F.R. § 39.7(d)(4).

[5] *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).

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

Ron Ciesiel General Manager Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 614-3265 (501) 821-8726 – facsimile rciesiel.re@spp.org Joe Gertsch Manager of Enforcement Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1672 (501) 821-8726 – facsimile jgertsch.re@spp.org SPP RE File Clerk Southwest Power Pool Regional Entity 201 Worthen Drive Little Rock, AR 72223 (501) 688-1681 (501) 821-8726 – facsimile spprefileclerk.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.	Sonia C. Mendonça* Vice President, Deputy General Counsel, and Director of Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Director of Enforcement Oversight 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 Alexander Kaplen* Associate Counsel North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile alexander.kaplen@nerc.net

Conclusion

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

Respectfully submitted,

/s/ Alexander Kaplen

Sonia C. Mendonça
Vice President, Deputy General Counsel, and Director of Enforcement
Edwin G. Kichline*
Senior Counsel and Director of Enforcement Oversight
Alexander Kaplen*
Associate Counsel
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.kichline@nerc.net
alexander.kaplen@nerc.net

cc: Unidentified Registered Entity
Southwest Power Pool Regional Entity