NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

July 28, 2016

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. NP16-_-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 SERC Reliability Corporation (SERC) and URE have entered into a Settlement Agreement to resolve all outstanding issues arising from SERC's determination and findings of 11 violations of 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 (2016). *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 neither admits nor denies the violations, but has agreed to the assessed penalty of two hundred twenty-five thousand dollars ($225,000), 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 SERC 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 (2016), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement.

*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
SERC2014013657	CIP-002-3	R3	High/ Severe	SR	Minimal	$225,000
SERC2014013877	CIP-005-1	R1	Medium/ Severe	CA	Moderate	
SERC2014013910	CIP-005-3a	R4	Medium/ Severe	CA	Minimal	
SERC2014014396	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014014403	CIP-006-3c	R8	Medium/ Severe	SR	Minimal	
SERC2014013881	CIP-007-3a	R5	Medium/ Severe	CA	Moderate	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method*	Risk	Penalty Amount
SERC2014014274	CIP-007-3a	R5	Medium/ Severe	SR	Minimal	$225,000
SERC2014013438	CIP-007-3a	R6	Lower/ Severe	SR	Moderate	
SERC2014013765	CIP-007-3a	R6	Lower/ Severe	SR	Minimal	
SERC2014013767	CIP-007-3a	R8	Medium/ Severe	SR	Moderate	
SERC2014013766	CIP-009-3	R5	Lower/ Severe	SR	Moderate	

SERC2014013657 CIP-002-3 R3 - OVERVIEW

SERC determined that URE did not develop a comprehensive list of all Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset in three instances. The first instance was due to URE's failure to document the asset on its network drawings upon commissioning or within 90 days. For the second and third instances, URE business units did not provide required data elements to the responsible personnel and were inconsistent in their classification of devices.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE's failure to document all CCAs on its CCA lists increased the risk that it would not afford those CCAs all the protections of the CIP Standards, which could allow a malicious individual to disrupt or misuse CCAs and thereby impair URE's situational awareness of the BPS. In the first instance, the device did not have control functions to operate key assets within the Critical Asset. The device communicated to the control center though a protected network that had monitoring and logging enabled. In addition, the device only provided analog and digital status updates with limited control functionality for reclosing breakers and backup ground relay protection. For the second and third instances, the CCAs that URE omitted from the CCA list had the required CIP security protections. Lastly, URE protected all of the CCAs URE omitted from the CCA list within Electronic Security Perimeters (ESPs) and Physical Security Perimeters (PSPs), and access was limited to authorized personnel who had taken cyber security training and had valid personnel risk assessments (PRAs).

SERC determined the duration of the violation to be from when URE commissioned the first device without identifying it as a CCA through when the senior manager updated and approved the CCA list.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove all control capabilities from the device so it is currently in a monitoring state only providing analog and digital statuses;
2. perform a walk-down to verify there are no additional CCAs that were installed and not properly identified;
3. perform a review of the Cyber Asset list to determine all of the Critical Asset locations;
4. perform a review of all ESP diagrams to confirm all CCAs are captured;
5. establish a standard operating procedure for identifying whether projects affect Critical Assets;
6. perform a review of the current information captured on all CCAs;
7. perform a review of the current process and identify updates to the current process for updating the CCA list;
8. identify the owners in the business unit/support groups responsible for maintaining the attributes on CCAs in their respective areas on a quarterly basis;
9. modify the CCA list to reflect the required fields needed for classification of the asset;
10. update the process to include the steps for the business unit/support group owners to follow; and
11. communicate the revised process to the business unit/support group representatives.

URE certified that it had completed its Mitigation Plan.

SERC2014013877 CIP-005-1 R1 - OVERVIEW

SERC determined that URE did not afford the protective measures specified in CIP-007 R3 to Cyber Assets used in the access control and/or monitoring of the ESP by failing to assess security patches on firewalls within 30 days of availability in two instances. URE had a subscription service with the firewall vendor for timely notification via email, however it had not received security patch updates from the vendor for several years due to an incorrect email address in the vendor site. URE did not follow up with the vendor or implement a secondary verification process to ensure that it received security patch notifications.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to assess security patches on the electronic access control and monitoring (EACM) devices at issue and subsequent failures either to install the security patches or implement compensating measures increased the risk that the EACM devices could be compromised, which could allow unauthorized electronic access to CCAs located within the ESP. Nevertheless, URE had an in-depth defense strategy of protection in which an intruder would first have to gain access through corporate firewalls to attempt access to the EACM devices at issue and avoid detection by an intrusion detection system. Further, the firewalls in question are located within PSPs. There were no known Cyber Security Incidents during the duration of the violation.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE assessed the missed security patches.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. verify that it is receiving security alerts from identified support vendors;
2. establish a communication link to receive advisory alerts;
3. update its IT security vulnerability management procedure;
4. identify the people who require training on the updated IT security vulnerability management procedure;
5. create training on the updated IT security vulnerability management procedure; and
6. deploy training on the IT security vulnerability management procedure.

URE certified that it had completed its Mitigation Plan.

SERC2014013910 CIP-005-3a R4 - OVERVIEW

SERC determined that URE did not document the plan to mitigate vulnerabilities identified during the annual Cyber Vulnerability Assessment (CVA). URE conducted its annual CVA and failed to identify that the network group or the firewall ruleset were no longer required because it had removed the devices from the network. URE's CVA process did not have enough detail to examine the deployed network objects or rulesets thoroughly.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to complete its CVA action plan to remove objects from the firewall rule group could allow unauthorized traffic to traverse the ESP. Nevertheless, the firewall rule containing

this group object was an outward-bound rule that only allowed communication out of the ESP and did not allow communication into the ESP. Further, the associated IP addresses were not associated with a network within the current ESP. The network group or configured firewall ruleset would not have allowed traffic to traverse the firewall and gain access to CCAs.

SERC determined the duration of the violation to be from the date when the network object and firewall ruleset were no longer required, through when URE implemented the approved change management removing the devices from the network object.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review and update the asset disposal and redeployment procedures;
2. create and deploy a change control and asset disposal or redeployment specific training program for personnel;
3. create a sub-task for the team to remove the machine name from the asset database; and
4. create sub-task for the system access sub-team to remove any specific firewall rules associated with a server to release the IP address for use by another system.

URE certified that it had completed its Mitigation Plan.

SERC2014014396 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not implement the technical and procedural controls for monitoring physical access at all access points to the PSP 24 hours a day, seven days a week. URE discovered that one of the PSP access points failed to provide "door forced open" and "door held open" alarms to the centralized security command center because of an equipment malfunction at the door contact.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor physical access at all PSP access points 24 hours a day, seven days a week could allow attempts at unauthorized physical access to CCAs within a PSP to go undetected. Nevertheless, the PSP door contacts were not functional for, at most, eight days. In addition, URE personnel are present in the PSP in question 24 hours a day, seven days a week. The PSP in question is located within a facility that has security on-site 24 hours a day, seven days a week with roving patrols. Upon discovering this issue, URE immediately deployed a security officer at the door until it repaired the door later that day. Although the door failed to provide the required alarms, it remained locked and only allowed authorized personnel access. URE performed a walk-down at all of its PSPs and determined that there were no other similar issues.

SERC determined the duration of the violation to be from the date the door contacts failed, through when URE repaired and tested the door contacts.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. provide training to the protective service employees responsible for PSP commissioning and validations;
2. update its PSP inspection checklists;
3. issue an emergency work order to repair the door contact; and
4. perform operability testing and return the door to full functionality.

URE certified that it had completed its Mitigation Plan.

SERC2014014403 CIP-006-3c R8 - OVERVIEW

SERC determined that URE did not perform testing and maintenance of all physical security mechanisms for one site on a cycle no longer than three years. URE utilizes a manual tool for tracking the maintenance and testing schedule. URE discovered that personnel mistakenly removed the PSP from view within the tool. Personnel had originally scheduled to remove the PSP from CIP scope prior to the next scheduled maintenance test.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to perform testing and maintenance of physical security mechanisms at least every three years could lead to URE being unaware of malfunctioning physical access control mechanisms, potentially allowing unauthorized individuals to gain physical access to CCAs. Nevertheless, URE secured the site with locking hardware and card readers and monitored 24 hours a day, seven days a week during the issue. In addition, the Cyber Assets deployed within the site in question were "low" upon implementing the CIP Version 5 impact rating criteria. URE performed additional operability testing on two occasions and determined that the physical access control systems were still operating as designed.

SERC determined the duration of the violation to be from three years and one day after URE conducted the last testing and maintenance of the physical security mechanisms at the site in question, through when URE updated its risk-based assessment methodology (RBAM) and removed the site from the Critical Asset list.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. decommission the PSP as a NERC CIP site;
2. conduct maintenance and testing for the site;
3. audit the existing maintenance and testing schedule to ensure all NERC CIP sites are listed and dates are accurate;
4. update the existing two procedural documents that support CIP-006-3c R8 to remove outdated information and incorporate current processes;
5. redesign the maintenance and testing tracking spreadsheet to include additional information needed for tracking and coordination with the business units;
6. retire and replace legacy/local procedures with new enterprise-wide procedures to ensure consistency in performing CIP-006-3c R8 maintenance and testing; and
7. retire the existing maintenance and testing checklist and revise to meet requirements of the new enterprise-wide procedures and ensure the document is complete and complies with CIP-006-3c R8.

URE certified that it had completed its Mitigation Plan.

SERC2014013881 CIP-007-3a R5 - OVERVIEW

SERC determined that URE did not change all default passwords on certain CCA and Critical Assets prior to deploying them within the ESP and failed to change each password at least annually. URE personnel were not familiar with the various levels of accounts available on the CCAs. Therefore, it did not know the accounts in question were present.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to change default passwords prior to putting CCAs in service could allow malicious individuals with knowledge of the default passwords to gain unauthorized electronic access to the CCAs. URE's subsequent failure to ensure that it changed passwords on the CCAs annually increased the risk that malicious individuals could compromise old passwords to gain unauthorized electronic access to the CCAs. Nevertheless, in order to access the default accounts, an individual would first have to login to the first-level account. Remote access to the CCAs was limited to individuals who had two-factor authentication configured and had the appropriate software application for successful interaction with the CCA. Remote access was not possible to the Cyber

Assets. The Cyber Assets were located within PSPs, which URE secures with badge readers and monitors access to 24 hours a day, seven day a week.

SERC determined the duration of the violation to be from the date when URE put the CCAs into service without changing the default passwords, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. update the current settings procedure to include language that outlines the need for an annual password reset for the specific devices and the steps to perform a password reset;
2. create a procedure that outlines the steps to be taken to perform an annual password update for the specific devices via remote access;
3. update the asset database list item field to include direction that the specific passwords need to be reset annually;
4. identify the list of people who required training and train on the updated setting procedure, the procedure for performing a password reset via remote access, and the change to the list item field to include direction that passwords need to be reset annually;
5. change all specific accounts' passwords during its annual password update;
6. perform a review of all assets to determine if any assets did not have an automatic password reset performed within 365 days;
7. create and document a procedure for performing a manual review of assets to determine whether an automated password reset has been performed; and
8. update the commissioning process document to direct the team to commission assets with unique asset names that have not been previously used.

URE certified that it had completed its Mitigation Plan.

SERC2014014274 CIP-007-3a R5 - OVERVIEW

SERC determined that URE did not implement its policy to secure shared accounts within seven days following personnel changes. URE did not configure its automated tool to change shared account passwords automatically. Therefore, URE was required to change the passwords manually. URE had a procedure in place stating the necessity to change shared account passwords manually, however URE personnel failed to follow it.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to change a password in a timely manner could have permitted unauthorized access to CCAs potentially resulting in damage and/or degradation of BPS reliability. Nevertheless, URE removed the logical access and physical access for the employee in question on the day of departure and changed the account password within ten days of the employee's departure. Prior to the voluntary departure, the employee was in good standing with URE, was current on training, and had a current PRA. URE verified that no changes occurred on the devices in question during the issue.

SERC determined the duration of the violation to be from eight days after the employee left URE and no longer required access to the shared account in question, through when URE manually changed the shared account password.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. manually change the shared account password;
2. identify individuals responsible for updating passwords to shared accounts; and
3. distribute the account management process to identified individuals to reeducate them on the importance of updating passwords to share accounts as documented in this policy.

URE certified that it had completed its Mitigation Plan.

SERC2014013438 CIP-007-3a R6 - OVERVIEW

SERC determined that URE did not implement automated tools or organizational process controls to monitor system events related to cyber security for all Cyber Assets within the ESP. Personnel did not understand the CIP logging requirements for the devices and thus did not configure them in the centralized security log-monitoring tool. Instead, personnel thought the devices were technically incapable of logging and would require filing TFEs. URE discovered additional CCAs that were not logging system cyber security events during its extent of condition review. URE personnel did not realize that for the second group of CCAs, it had to request that its vendor create rules to allow communication with the logging tool.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to monitor system events related to cyber security for the devices could have resulted in a security breach going undetected or impaired a response to a possible or actual security breach. An undetected security breach could render CCAs inoperable, resulting in the loss of monitoring and control of the BPS. Nevertheless, the CCAs have no direct control over the BPS.

Access to the Cyber Assets involved in this violation is limited to individuals with authorized physical or electronic access rights, and URE protects the Cyber Assets within an ESP and a PSP. In addition, URE has an intrusion detection system that monitors the network and alerts personnel in the event of unusual activity. URE did not discover or detect any cyber security events, Misoperations, emergencies, or other adverse consequences because of this violation.

SERC determined the duration of the violation to be from the date URE began installing the devices without implementing automated tools or organizational process controls to monitor system events related to cyber security, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. identify the resources that would require re-training of the asset commissioning process;
2. update documentation to include testing;
3. identify list of personnel requiring training on the updated procedures;
4. update and submit TFEs for relevant devices;
5. test devices; and
6. notify staff and conduct training.

URE certified that it had completed its Mitigation Plan.

SERC2014013765 CIP-007-3a R6 - OVERVIEW

SERC determined that URE did not implement automated tools to monitor system events related to cyber security for all Cyber Assets within the ESP and did not submit a request for a TFE to SERC that documented compensating measures. URE discovered CCAs at a single facility that were technically incapable of monitoring or logging cyber security events. URE maintained evidence from the vendor that the CCAs were not capable of logging or monitoring events related to cyber security. Nevertheless, URE failed to submit a request for a TFE to SERC that documented compensating measures.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to submit a request for a TFE documenting compensating measures for CCAs that were technically incapable of monitoring or logging cyber security events could have led URE to not document or implement compensating measures to protect the devices at issue, which could result in a security breach going undetected. Nevertheless, URE had implemented compensating measures

that included intrusion detection and protection systems monitoring for abnormal or malicious network traffic that were in place when it commissioned the CCAs. URE deployed CCAs within a PSP and ESP behind multiple firewalls. URE did not discover or detect any cyber security events, Misoperations, emergencies, or other adverse consequences because of this issue.

SERC determined the duration of the violation to be from the date when URE commissioned the CCAs that were technically incapable of monitoring or logging cyber security events without submitting a request for a TFE that documented compensating measures, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. remove the facility from scope with a new RBAM utilizing new criteria; and
2. implement a new TFE program and train the TFE audience.

URE certified that it had completed its Mitigation Plan, and SERC verified that URE had completed all mitigation activities.

SERC2014013767 CIP-007-3a R8 - OVERVIEW

SERC determined that URE did not perform CVAs of all Cyber Assets within its ESPs at least annually. URE discovered CCAs within its Cyber Assets that contained a connection with the supervisory control and data acquisition (SCADA) wide area network. URE personnel did not understand that the CVA requirements applied to these Cyber Assets connected to the CCA.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to perform a CVA on Cyber Assets in its facilities could have left the Cyber Assets residing within ESPs open to potential security threats and compromise for an extended period. Nevertheless, URE logically separated the local area network from the SCADA network, and the Cyber Assets resided within secured ESPs and PSPs. Remote access to the Cyber Assets from outside the ESP required two-factor authentication. In addition, URE's electronic access and control monitoring devices did not identify any malicious activity during the violation that would have affected the involved Cyber Assets. URE restricted access to the Cyber Assets to authorized individuals with completed PRAs and cyber security training.

SERC determined the duration of the violation to be from the date it commissioned the first site, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. review documents listing all of the existing ports;
2. perform a CVA on all Cyber Assets during the annual walk-downs;
3. initiate testing of full-time CVA scans in a test lab; and
4. draft engineering configuration/settings and designs to implement a new CVA process.

URE certified that it had completed its Mitigation Plan.

SERC2014013766 CIP-009-3 R5 - OVERVIEW

SERC determined that URE did not annually test information essential to recovery that is stored on backup media to ensure that the information is available for the CCAs at one facility. URE's subject matter expert had misunderstood the requirement, believing it was sufficient to create frequent backup tapes throughout the year, instead of testing the tapes to ensure the information was readable. URE's disaster recovery procedure implemented at the site required annual testing of the backup media.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to test backup media necessary to recover CCAs could result in it being unaware that the information was corrupted, possibly delaying or preventing the restoration of CCAs. Nevertheless, this violation affected a single site and thus would have a limited effect in the event that URE needed to recover the CCAs at the site. URE performed frequent backups of the information necessary to recover the CCAs and performed monitoring of the backup system. No Misoperations, emergencies, or other adverse consequences occurred during the period of the violation.

SERC determined the duration of the violation to be from the date URE commissioned the CCAs at the facility without testing the information essential to recovery to ensure it was available, through when URE completed its Mitigation Plan.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to:

1. gather lessons learned and conduct training to ensure individual subject matter experts understand the requirements and processes that are outlined to be compliant with this requirement; and

2. perform training and lessons learned gathered with individuals reviewing work management tickets that are created to initiate the completion of this requirement.

URE certified that it had completed its Mitigation Plan.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of two hundred twenty-five thousand dollars ($225,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. SERC determined the compliance history should serve as an aggravating factor;
2. SERC considered certain elements of URE's internal compliance program (ICP) as a mitigating factor in the penalty determination. Specifically, URE's ICP is documented and readily available to its employees on its intranet. A URE compliance group reviews its ICP on an annual basis, which reports within URE's compliance department to ensure independence from the operations and engineering departments that must comply with the NERC Standards. URE employees receive quarterly newsletters to ensure awareness of ethics and compliance issues and annual CIP training. URE employees are also required to understand all corporate policies and procedures, including those related to compliance, and are subject to discipline, up to and including termination, for violating those policies. Nevertheless, SERC reduced ICP credit due to URE's compliance history and inability to prevent recurrence of CIP issues.
3. URE voluntarily self-reported eight of the violations; however, five of the Self-Reports came after notice of an upcoming Compliance Audit, and therefore did not receive mitigating credit;
4. URE was cooperative throughout the compliance enforcement process;
5. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
6. six of these violations posed minimal risk and five violations posed moderate risk and did not pose a serious or substantial risk to the reliability of the BPS; and
7. there were no other mitigating or aggravating factors or extenuating circumstances that would affect the assessed penalty.

After consideration of the above factors, SERC determined that, in this instance, the penalty amount of two hundred twenty-five thousand dollars ($225,000) is appropriate and bears a reasonable relation to the seriousness and duration of the violations.

Prior to starting settlement discussions, SERC initiated meetings with URE compliance staff and middle management to discuss the high number of URE violations and the issues SERC was seeing with URE's compliance efforts. SERC management met with URE senior management after settlement discussions began to continue the discussion of SERC's concerns. To address SERC's concerns, URE met with SERC after reaching a settlement agreement to inform SERC of a comprehensive action plan that included the following elements:

1. The creation of an internal board, to ensure adequacy of cause and extent of condition analyses and review effectiveness of mitigation plans;

2. Enhanced oversight by an internal committee, along with enhanced reporting to provide members with immediate notification of possible violations;

3. Enhanced mitigation plan tracking at the enterprise level to allow for regular status reporting;

4. Quarterly meetings with SERC to discuss progress and solicit feedback;

5. The review and enhancement of URE's communication plan to educate business continually on the company's approach to ensure NERC compliance; and

6. The establishment of additional program objectives and metrics, as required.

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 July 14, 2016 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.

---

[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).

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of two hundred twenty-five thousand dollars ($225,000) 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.

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

James M. McGrane* Managing Counsel – Enforcement SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7787 (704) 357-7914 – facsimile jmcgrane@serc1.org Drew R. Slabaugh* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 414-5244 (704) 357-7914 – facsimile dslabaugh@serc1.org Gary Taylor* President and Chief Executive Officer SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 940-8205 (704) 357-7914 – facsimile gtaylor@serc1.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 of Enforcement and Deputy General 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 G. Kichline* Senior Counsel and Associate Director, Enforcement 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 Leigh Anne Faugust* Counsel, Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile leigh.faugust@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/ Edwin G. Kichline
Sonia C. Mendonça
Vice President of Enforcement and Deputy General Counsel
Edwin G. Kichline
Senior Counsel and Associate Director, Enforcement
Leigh Anne Faugust
Counsel, 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.kichline@nerc.net
leigh.faugust@nerc.net

cc: Unidentified Registered Entity
SERC Reliability Corporation