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 14 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 one hundred eighty thousand dollars ($180,000), 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* Date	Risk	Penalty Amount
SERC2014014337	CIP-003-3	R4	Medium/ Severe	SR	Minimal	$180,000
SERC2014014336	CIP-003-3	R5	Lower/ Severe	SR	Minimal	
SERC2014014086	CIP-005-1	R1	Medium/ Severe	SR	Moderate	
SERC2014014427	CIP-005-3	R3	Medium/ Severe	SR	Moderate	
SERC2014014196	CIP-005-3a	R4	Medium/ Severe	SR	Minimal	
SERC2014013621	CIP-006-1	R1	Medium/ Severe	SR	Minimal	
SERC2014013444	CIP-006-3c	R1	Medium/ Severe	SC	Minimal	

NERC Violation ID	Standard	Req	VRF/ VSL	Discovery Method* Date	Risk	Penalty Amount
SERC2014014195	CIP-006-1	R2	Medium/ Severe	SR	Minimal	$180,000
SERC2014014198	CIP-006-3c	R2	Medium/ Severe	SR	Moderate	
SERC2014013437	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014014395	CIP-006-3c	R5	Medium/ Severe	SR	Minimal	
SERC2014013619	CIP-007-1	R5	Medium/ Severe	SR	Minimal	
SERC2014014423	CIP-007-1	R5	Lower/ Severe	SR	Minimal	
SERC2014014087	CIP-007-1	R6	Lower/ Severe	SR	Moderate	

SERC2014014337 CIP-003-3 R4 - OVERVIEW

SERC determined that URE did not fully implement its program to identify, classify, and protect information associated with Critical Cyber Assets (CCAs).

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 identify, classify, and protect CCA information repositories could allow unauthorized individuals access to CCA information. Nevertheless, although URE had not identified or maintained the CCA information repositories, its affiliate had identified the repositories and protected them as required. Personnel with access to the CCA information repositories were authorized. In addition, a malicious individual could not gain direct access to CCAs by gaining access to CCA information.

SERC determined the duration of the violation to be from the date URE incompletely implemented an update to its CIP compliance program, 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 and document the URE repositories that contained CCA information;
2. ensure that access reviews for all repositories were reviewed under a compliance program;
3. complete the annual repository review;
4. research whether any additional repositories exist and add them to the repository list and perform the annual repository reviews as required; and
5. update policies/procedures to accept the lists and reviews done on repositories containing CCA information as part of the annual review to avoid duplication and relying on the existing access controls used for all repositories.

URE certified that it had completed its Mitigation Plan.

SERC2014014336 CIP-003-3 R5 - OVERVIEW

SERC determined that URE did not review at least annually the access privileges to protected CCA information in two instances. Failure of process ownership, human error, and employee turnover were the primary causes of this violation.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Failure to review the repositories annually could result in individuals having access to CCA information past the time such access is required. Such individuals could use CCA information to plan or coordinate attacks on CCAs. Nevertheless, URE regulates the access to the affected repositories based on physical and electronic access and grants access only to authorized personnel. URE has controls that remove physical and electronic access as part of its standard off-boarding procedure. URE would have removed access for any terminated individuals leaving during the time of the issue, minimizing the possibility of unauthorized personnel with access.

SERC determined the duration of the violation to be from the first day URE failed to complete the annual access review, through when URE completed its next annual access review.

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

1. receive responses from repository owners regarding repository access;

2. update work level instructions regarding gathering and documenting responses that have been updated by the individuals who have been assigned to do that activity in order to meet current needs;
3. provide a notification email to the manager and individuals involved with the gathering of approvals for the annual review; and
4. test and update work-level instructions created for the missed review if required during the next review.

URE certified that it had completed its Mitigation Plan.

SERC2014014086 CIP-005-1 R1 - OVERVIEW

SERC determined that URE did not afford the protections of CIP-007 R1, R3, R4, R5, R6, and R8 to all Cyber Assets used in the Electronic Access Control and/or Monitoring (EACM) of the Electronic Security Perimeter (ESP) in seven instances. The instances were due to: 1) failures to follow documented procedures; 2) employee turnover; 3) inadequate transitioning of responsibilities; 4) failures to document changes adequately; 5) inadequate account review processes; 6) inadequate procedures; and 7) failure to notify asset owners.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to provide EACM devices the protective measures specified in CIP-007 R1, R3, R4, R5, R6, and R8 could leave EACM devices exposed to known vulnerabilities for an extended period. Nevertheless, several factors reduced the risk of the violation. For the CIP-007 R1 failure, URE authorized the changes that it did not properly document and implemented the changes using its documented change management procedure. For the CIP-007 R4 failure, URE had earlier versions of antivirus signatures running, providing protection against some viruses and malware. For the CIP-007 R5.1.3 failures, URE has controls that remove electronic access as part of its standard off-boarding procedure, and any terminated individuals leaving URE would have had their access revoked even if they still had an account on a specific EACM device not removed as required. For the CIP-007 R5.3.3 failures, URE determined that no one accessed the accounts in question after the passwords expired, and existing controls would force an individual trying to access the accounts to change the passwords. In addition, URE protected its EACM devices within Physical Security Perimeters (PSPs) and behind corporate firewalls that require two-factor authentication through a restricted VPN to access remotely.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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 the active directory domain accounts to determine what accounts require a password reset, access removal, or Technical Feasibility Exception (TFE);
2. remove access to accounts deemed to no longer need their access either based on infrequent use or access of account determined to no longer be required;
3. reset the passwords on the accounts which still require access;
4. create a new process that will detect and change passwords automatically to ensure they do not exceed a year in time unless a TFE is required for the account;
5. document the new process as part of energy management and process control systems team's policies and procedures; and
6. communicate the policy/procedure change to the affected parties.

URE certified that it had completed its Mitigation Plan.

SERC2014014427 CIP-005-3 R3 - OVERVIEW

SERC determined that URE did not implement monitoring, logging, and alerting at all access points to the ESP 24 hours a day, seven days a week. The root cause of the violation was human error. Upon completion of a hardware replacement project, URE personnel reviewed firewall traffic to determine if URE was monitoring and logging all the Cyber Assets. However, URE should have reviewed the documented list of deployed Cyber Assets instead.

SERC determined that this violation posed a moderate and not serious or substantial risk to the reliability of the BPS. URE's failure to implement logging or alerting at electronic access points to the ESP could result in unauthorized access and/or unauthorized access attempts going undetected. Nevertheless, URE had configured the devices to deny traffic by default and went through Cyber Vulnerability Assessments (CVAs) to validate that it had enabled only the ports and services required for operations.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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 devices in scope;
2. verify devices are configured to send logs to the monitoring program;
3. verify monitoring program receives logs and maintains for 90 days;
4. develop a report that lists all devices that are logging and compare that against list of devices in inventory;
5. develop plan to implement a monitoring script that detects when logging fails for a device;
6. implement a monitoring script to ensure notification in the event monitoring fails;
7. implement a manual log review if logging/monitoring is unavailable;
8. validate that alerting rules are properly configured for affected devices; and
9. communicate and train on the new manual logging process.

URE certified that it had completed its Mitigation Plan.

SERC2014014196 CIP-005-3a R4 - OVERVIEW

SERC determined that URE did not document the execution status of its annual CVA action plans for electronic access points. SERC determined URE failed to include adequate procedures for ensuring its personnel updated the remediation action plans in a timely manner.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to take action on vulnerabilities identified during a CVA could allow malicious individuals to exploit known vulnerabilities in order to gain access to CCAs and other Cyber Assets. Nevertheless, the electronic access points (EAPs) at issue were virtual private networking devices utilized to secure communications between two remote locations, and did not allow direct access to CCAs. A PSP protected the EAPs.

SERC determined the duration of the violation to be from the date URE documented its action plans to remediate vulnerabilities identified in its CVA, through when URE updated the status of the CVA action plan for the open items.

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

1. update the status column on the Mitigation Plan tab for all open items on the spreadsheet;
2. transition EAP assets to IT security who will track CVA statuses and remediation and update documentation;
3. follow IT security procedures that prescribe how CVA tracking and documentation is performed and how follow-up is to occur for the remediation action plan after it is created and initial contact with the asset owner is made;
4. show evidence of CVAs performed or timeline for performing CVAs on respective EAP assets; and
5. train on procedures that prescribe how CVA tracking and documentation is performed.

URE certified that it had completed its Mitigation Plan.

SERC2014013621 CIP-006-1 R1 - OVERVIEW

SERC determined that URE did not establish a completely enclosed (six-wall) border and it did not have alternative measures deployed nor documented at a PSP. URE discovered four holes in the back of a closet within a PSP. The openings within the closet would have led to an area designated as a non-PSP area. URE used a process to commission PSPs that was not robust and URE did not implement a rigorous process that required a thorough inspection of PSP boundaries.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to ensure that all Cyber Assets within an ESP reside completely within a six-wall border PSP could have allowed unauthorized individuals to gain physical access to CCAs. Nevertheless, the PSP is within a protected building secured by security cameras, contracted security personnel, and badge-access entry points, making it difficult for unauthorized individuals to gain access to the PSP. In addition, URE personnel staff the PSP 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE sealed the four holes in the PSP.

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

1. bolt the closet door shut;

2. update the PSP diagram to include the closet;
3. seal four holes by installing solid aluminum plating with screws from inside the PSP closet and with screws epoxied from outside the PSP;
4. inspect legacy sites;
5. perform an evaluation and complete repair of alarm on a door at a legacy site;
6. provide training to employees responsible for commissioning and PSP validation; and
7. update the checklists used for the PSP inspection process.

URE certified that it had completed its Mitigation Plan.

SERC2014013444 CIP-006-3c R1 - OVERVIEW

SERC determined that URE did not implement its documented visitor control program for continuous escort of visitors and logging visitor access to a PSP. The visitor was unescorted for approximately 15 minutes while repairing a printer and had not completed the necessary visitor access log.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to escort a visitor within a PSP and ensure that the visitor signed the visitor access log could have enabled the visitor to tamper with or physically damage CCAs without a record of them being in the PSP. Nevertheless, the visitor's access was limited to a room that did not contain CCAs. The CCAs were within an inner room and secured by additional doors that required badge access that the visitor did not possess. The visitor did not enter that room. In addition, URE personnel continually staffed the PSP containing the CCAs during the time that the visitor was unescorted.

SERC determined the duration of the violation to be from when the URE staff stopped escorting the visitor, through when the visitor left the PSP.

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

1. provide coaching to the employee-contractor on visitor control;
2. implement physical security posters with security requirements and procedures; and
3. conduct staff meetings with the business units and review and reinforce the requirements of the CIP PSP visitor control program to continuously escort visitors and to have escorts require visitors to sign in and complete the visitor access log.

URE certified that it had completed its Mitigation Plan. SERC verified completion of URE's Mitigation Plan.

SERC2014014195 CIP-006-1 R2 - OVERVIEW

SERC determined that URE did not implement the operational and procedural controls to manage physical access at all access points to the PSPs 24 hours a day, seven days a week at three locations. The first location was an unsecured vent hatch; the second location was a small, energized space with a high risk of electrocution; and the third granted access to an airshaft. The root cause was insufficient training for personnel inspecting PSPs.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to properly manage physical access at access points to the PSP using one of the access control methods authorized by CIP-006 R2 could allow unauthorized individuals to gain access to CCAs without being detected, allowing them to tamper with or destroy CCAs. Nevertheless, the access points at the first and third location were alarmed. The alarms would have alerted the appropriate monitoring workstation for a response in the event someone opened the access points—URE received no such alerts during the violation period. At the second location, an intruder would have gained access to a small space and risked electrocution to gain access to CCAs. In addition, the access points at the first and second locations were within secure facilities that URE personnel staffed and security guards monitored 24 hours a day, seven days a week.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, 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. provide training to employees responsible for validating the PSP;
2. update the checklists used for the PSP inspection process;
3. permanently secure both sides of the metal bars to restrict access through the ventilation hatch at the third location;
4. install pad locks on all of the exterior doors at the second location;
5. put a roving patrol in place to ensure the doors in question were still locked and secured; and
6. install a hatch door at the first location.

URE certified that it had completed its Mitigation Plan.

SERC2014014198 CIP-006-3c R2 - OVERVIEW

SERC determined that URE did not afford the protective measures specified in CIP-007 R5.1.3 and R5.3.3 to Cyber Assets that authorize and/or log access to a PSP in two instances. The first instance was one user account on URE's Physical Access Control System (PACS) exceeded the annual password change requirement. The second instance was a failure to perform a first quarter review of authorized user accounts. The root cause was a failure to put controls in place to force password resets and premature implementation of controls that delayed an employee from having necessary access to generate the report for the first quarter review.

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 passwords on PACS on an annual basis and its failure to perform quarterly access reviews for PACS accounts could give malicious individuals additional time and opportunities to compromise PACS devices, allowing them to make unauthorized modification to physical access rights to CCAs. Nevertheless, access to the PACS requires either physical access, or logical access and two-factor authentication. No one had used the PACS account with the expired password in more than 120 days, which had caused the account to lock, requiring a password change upon the next login. A locked account requires administrator intervention after 120 days of inactivity, requiring a system administrator to reset the password. The account owner had a current personnel risk assessment (PRA) and attended the required cyber security training. For the user account review issue, URE has documented controls and procedures that remove physical and electronic access to Cyber Assets when appropriate, reducing the risk that an individual that should have been removed from the access list would retain the ability to access the PACS.

SERC determined the duration of the violation to be from the first day after the year in which URE did not change the PACS password, 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. contact the account owner in order to work with the administrator to change the password;
2. transition support for device where the account with expired password resides;
3. create a new process that will detect and change passwords if an account has passed a pre-determined limit of days since the last password change;
4. document the change as part of policies and procedures; and
5. communicate the policy/procedure change to the affected parties.

URE certified that it had completed its Mitigation Plan.

SERC2014013437 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not immediately review and respond to a single unauthorized physical access attempt alarm in accordance with URE procedures during a 26-hour period when communications were down. The violation was due to a failure on the part of URE personnel to follow established procedures for notification.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE failed to review and respond immediately to a received unauthorized access attempt alarm at one site during a 26-hour period when communications were down. Nevertheless, the card readers at the site continued to operate in a stand-alone mode during the loss of communications. All access and alarm activity cached at the card reader and downloaded to the server once the communication resumed. During this period, URE should have responded to one unauthorized access attempt alarm—URE handled the alarm appropriately after communication resumed. URE confirmed no individuals without authorization gained access to the site during this period. The site is protected by security fencing, security guards that monitor the site 24 hours a day, seven days a week, electronic access controls, and video cameras.

SERC determined the duration of the violation to be from when URE first lost communications with its alarm systems at one PSP, through when URE deployed security guards to monitor physical access to the PSP.

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

1. issue an email to all supervisors and personnel providing details of the incident and the errors made;
2. issue disciplinary action notices to the three personnel and three shift supervisors who were involved in this incident;
3. develop a procedure for staff relief for the NERC regulated desk;
4. evaluate the training program, determine if any gaps exist, and develop a list of enhancements; and
5. update and perform the formal training program for relevant personnel.

URE certified that it had completed its Mitigation Plan.

SERC2014014395 CIP-006-3c R5 - OVERVIEW

SERC determined that URE did not implement controls to monitor access at all access points to the PSP. A remote facility experienced a loss of air conditioning and informed the command center that personnel would be propping open the door to maintain an acceptable temperature. A URE employee observed that the door to the PSP was propped open without a guard continuously monitoring the access point. The employee then notified security, which posted a guard at the access point.

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 to the PSP at issue could have allowed unauthorized individuals to gain physical access to and tamper with or destroy the CCAs inside. Nevertheless, URE deployed security guards on roving patrols that checked the PSP access point on an hourly basis starting when personnel first propped open the door. The guards continued the roving patrols until a guard posted to the PSP access point. The facility was located within a complex with personnel onsite 24 hours a day, seven days a week. In addition, a security fence with guards posted at the front gate secures the complex. Once URE identified the issue, a guard monitored the open door until the issue was resolved.

SERC determined the duration of the violation to be for approximately two and a half days when the PSP door was propped open without ensuring continuous monitoring.

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

1. post a continuous monitoring guard at the propped open door until the door could be closed; and
2. send out an email to operations teams at the facility reminding them of the site-specific physical security plan that details the procedure for how to monitor propped open doors in a PSP.

URE certified that it had completed its Mitigation Plan.

SERC2014013619 CIP-007-1 R5 - OVERVIEW

SERC determined that URE did not annually change 11 account passwords associated with CCAs. URE had a technical password control deployed to force a password change after 365 days, but the control would only force a password change if there were an attempted login.

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 account passwords annually could leave Cyber Assets vulnerable to compromise through unauthorized use of an old password. Nevertheless, URE reviewed access logs and determined that no one had accessed the accounts in question since the date of password expiration. If an individual tried to access an account, the controls would have forced a password change. This issue affected two sites. PSPs and ESPs protected all affected Cyber Assets.

SERC determined the duration of the violation to be from the first day URE should have annually changed passwords, through when URE changed all passwords and filed a TFE for an account password that it could not change annually.

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

1. expand password review to other registrations;
2. delete, disable, or change passwords on all of the affected accounts with one exception;
3. file a TFE for the one exception account;
4. review CVAs from its sites to assess its compliance with CIP-007-3c R5.3.3; and
5. develop preventive maintenance task to review password age of Cyber Assets.

URE certified that it had completed its Mitigation Plan. SERC verified completion of URE's Mitigation Plan.

SERC2014014423 CIP-007-1 R5 - OVERVIEW

SERC determined that URE did not document mitigating measures for Cyber Assets that could not technically enforce the password complexity requirement and did not submit a request for a TFE. The violation was limited to only one facility and was due to personnel failing to follow documented procedures to document compensating measures by filing for TFEs for Cyber Assets when appropriate.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE's failure to follow its procedures to document compensating measures by filing a TFE when Cyber Assets were not technically capable of enforcing password complexity requirements increased the risk of unauthorized access to Cyber Assets within the ESP. Nevertheless, although it could not technically enforce the password complexity requirements on the Cyber Assets at issue, URE

checked the passwords and confirmed that they met the password complexity requirements, as required by its documented procedures. In addition, URE kept the Cyber Assets within a secure PSP and ESP, and all users had valid PRAs and cyber security training.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE filed its TFE with SERC.

URE submitted its Mitigation Plan to address the referenced violations. URE's Mitigation Plan required URE to file a TFE for these devices for CIP-007-3 R5.3.

URE certified that it had completed its Mitigation Plan.

SERC2014014087 CIP-007-1 R6 - OVERVIEW

SERC determined that URE did not implement automated tools or organizational process controls to monitor system events related to cyber security. URE discovered that the centralized logging and monitoring system was not receiving cyber security events for CCAs. SERC determined the primary cause of the violation was the lack of procedural and technical controls to assess whether URE was monitoring cyber security events for all Cyber Assets within the ESP.

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 all Cyber Assets within the ESPs could have resulted in signs of a security breach going undetected. In addition, URE's failure to log system events related to security events could have impaired its ability to conduct an incident response. Nevertheless, this violation was limited to CCAs located at a single site. URE deployed an intrusion detection system to monitor the network on which the affected CCAs reside, and the CCAs resided within a PSP. URE did not discover or detect any cyber security events, Misoperations, or other adverse consequences because of the violation. Finally, URE could have reviewed the logs if an event occurred.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable, through when URE corrected the settings on the domain-based firewall to allow the centralized logging and monitoring system to collect the event logs.

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

1. remediate all devices by changing a configuration in a group policy;

2. update the CCA checklist to include steps to review logs manually in the event of a logging and monitoring device outage for any reason;
3. communicate the updated changes to the CCA checklist to the responsible individuals;
4. update the security status monitoring procedure;
5. communicate the updated changes to the security status monitoring procedure; and
6. perform a root cause analysis.

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 one hundred eighty thousand dollars ($180,000) 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 13 of the violations; five of the Self-Reports, however, 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. ten of these violations posed minimal risk and four 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 one hundred eighty thousand dollars ($180,000) 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.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of one hundred eighty thousand dollars ($180,000) 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:

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 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 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