PRIVILEGED AND CONFIDENTIAL INFORMATION HAS BEEN REMOVED FROM THIS PUBLIC VERSION

February 26, 2015

VIA ELECTRONIC FILING

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

Re: NERC Full Notice of Penalty regarding Unidentified Registered Entity, FERC Docket No. NP15-_-000

Dear Ms. Bose:

The North American Electric Reliability Corporation (NERC) hereby provides this Notice of Penalty[1] regarding Unidentified Registered Entity (URE), NERC Registry ID# NCRXXXXX, in accordance with the Federal Energy Regulatory Commission's (Commission or FERC) rules, regulations, and orders, as well as NERC's Rules of Procedure including Appendix 4C (NERC Compliance Monitoring and Enforcement Program (CMEP)).[2]

This Notice of Penalty is being filed with the Commission because 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 the violations[3] addressed in this Notice of Penalty. According to the Settlement Agreement, URE neither admits nor denies the violations, but has agreed to the assessed penalty of seventy thousand dollars ($70,000), in addition to other remedies and actions to mitigate the instant violations and facilitate future compliance under the terms and conditions of the

[1] *Rules Concerning Certification of the Electric Reliability Organization; and Procedures for the Establishment, Approval, and Enforcement of Electric Reliability Standards* (Order No. 672), III FERC Stats. & Regs. ¶ 31,204 (2006); *Notice of New Docket Prefix "NP" for Notices of Penalty Filed by the North American Electric Reliability Corporation*, Docket No. RM05-30-000 (February 7, 2008). *See also* 18 C.F.R. Part 39 (2014). *Mandatory Reliability Standards for the Bulk-Power System*, FERC Stats. & Regs. ¶ 31,242 (2007) (Order No. 693), *reh'g denied*, 120 FERC ¶ 61,053 (2007) (Order No. 693-A). *See* 18 C.F.R § 39.7(c)(2).

[2] *See* 18 C.F.R § 39.7(c)(2) and 18 C.F.R § 39.7(d).

[3] For purposes of this document, each violation at issue is described as a "violation," regardless of its procedural posture and whether it was a possible, alleged, or confirmed violation.

Settlement Agreement. Accordingly, the violations in this Full Notice of Penalty are being filed in accordance with the NERC Rules of Procedure and the CMEP.

Statement of Findings Underlying the Violations

This Notice of Penalty incorporates the findings and justifications set forth in the Settlement Agreement and disposition documents. The details of the findings and basis for the penalty are set forth in the Settlement Agreement and herein. This Notice of Penalty filing contains the basis for approval of the Settlement Agreement by the NERC Board of Trustees Compliance Committee (NERC BOTCC). In accordance with Section 39.7 of the Commission's regulations, 18 C.F.R. § 39.7 (2014), NERC provides the following summary table identifying each violation of a Reliability Standard resolved by the Settlement Agreement, as discussed in greater detail below.

NERC Violation ID	Reliability Std.	Req.	VRF/VSL*	Total Penalty
SERC2013012689	CIP-002-1	R3	High/ Severe	$70,000
SERC2013012691	CIP-005-1	R1; R1.1; R1.5	Medium/ Severe	
SERC2014013574	CIP-005-1	R1; R1.4	Medium/ Severe	
SERC2013011676	CIP-005-1	R3	Medium/ Severe	
SERC2013011702	CIP-006-3c	R1; R1.1; R1.6	Medium/ Severe	
SERC2013012693	CIP-006-1	R3	Medium/ Severe	
SERC2013012695	CIP-007-1	R1	Medium/ Severe	
SERC2013012694	CIP-007-1	R2: R2.1	Medium/ Severe	
SERC2012009565	CIP-007-1	R3	Lower/ Severe	
SERC2012009647	CIP-007-1	R4	Medium/ Severe	
SERC2012009566	CIP-007-1	R5; R5.2; R5.3	Medium/ Severe	
SERC2012009564	CIP-007-1	R6	Medium/ Severe	

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

CIP-002-1 R3 (SERC2013012689)

During a Compliance Audit, SERC determined that URE failed to develop a complete list of Critical Cyber Assets (CCAs) essential to the operation of a Critical Asset. Specifically, URE failed to identify network switches as CCAs. URE used the switches between their modem banks and the terminal servers within its Energy Management System (EMS). The data traversing the switches provided real-time operational decision-making information and situational awareness. URE had identified and protected the switches as Cyber Assets within the Electronic Security Perimeter (ESP).

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the bulk power system (BPS). URE was affording the switches all the protections it provided to other CCAs and non-critical Cyber Assets within the ESP. Namely, the switches were behind firewalls in an ESP and surrounded in a six-wall enclosed Physical Security Perimeter (PSP). For those requirements for which the devices were unable to comply, there was an approved Technical Feasibility Exception (TFE) in place.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. performed a gap analysis to ensure it had properly classified all devices properly based on the present violation;
2. updated the CIP-002 list to show these devices;
3. ensured the senior manager approved the updated list; and
4. updated the ESP drawing to show the devices.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1 (SERC2013012691)

During a Compliance Audit, SERC determined that URE failed to identify all access points and Cyber Assets within the ESP. Specifically, URE failed to identify serial switches and one electronic access point (EAP) providing access to administrator workstations as access points to an ESP. The serial switches allow serial communications to traverse the ESP and communicate with the EMS. URE had

classified the devices as Cyber Assets within the ESP and protected them as such. The EAP at issue (a domain controller) was configured to allow virtual private network access from the corporate network and allowed remote personnel full administrative access on the ESP.

In addition, URE failed to identify an electronic access control and monitoring system and afford it the protective measures specified in CIP-005-3a R1.5. URE performed an EMS upgrade and failed to remove the domain controller from the ESP network.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to identify all access points and to protect Cyber Assets within the ESP could have resulted in vulnerabilities that allow a potential attacker to access and compromise systems within the ESP. Several factors mitigated the risk. First, the domain controller that remained within the ESP did not perform electronic access control for the newly deployed EMS. Second, URE has logging and monitoring enabled devices within the ESP that would have detected possible intrusion. Third, access to the devices was limited to authorized personnel who had completed cybersecurity training and had valid personnel risk assessments (PRAs). Finally, URE has a policy that prohibits personnel from connecting remotely to perform operational EMS functions.

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

URE's Mitigation Plan required URE to:

1. close all of the open network switch ports at all of its locations;
2. perform a gap analysis and update all of the required documents;
3. verify that all ports are monitored and alerted;
4. decommission the domain controller;
5. update the CIP-002 lists, which would then be approved by the senior manager;
6. test the switches for logging and alerting;
7. create a checklist for commissioning and decommissioning devices;
8. review the checklist with the appropriate personnel; and
9. design and implement an intermediate system.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R1.4 (SERC2014013574)

URE submitted a Self-Report stating that it had failed to identify and protect all non-critical Cyber Assets within the ESP. During an internal review, URE discovered that it had not identified a printer and a tape library located within the ESP as Cyber Assets and therefore had not protected them under CIP-005-1 R1.4. The printer was in production before the date the Standard became mandatory and enforceable. URE added the tape library to the Cyber Asset list, protecting the device with compensating measures under CIP-005, removed the tape library from the inventory list 10 months later, but did not remove it from use. URE later determined that the tape library was required for proper management of backups and it remained in use; however, URE never added it back to the inventory list.

SERC determined that URE was in violation of CIP-005 R1.4 because it failed to identify and protect all non-critical Cyber Assets within the ESP.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. Compensating measures for the tape library remained in place during the entirety of the violation. The devices were peripherals that assist with user access and functionality but that could not affect the reliable operation of the BPS or perform any other essential functions within the ESP.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. created recurring tasks to review ports and services for the devices;
2. updated the Cyber Asset Inventory list to include the devices;
3. reviewed ports and services for the devices;
4. created a device commissioning checklist for devices installed in the ESP;
5. developed a process to scan periodically the network to determine if a device has been added or removed from inside the ESP;
6. tested and then implemented the new process;

7. reviewed security updates for each device;
8. applied all applicable updates; and
9. decommissioned the printer.

URE certified that the above Mitigation Plan requirements were completed.

CIP-005-1 R3 (SERC2013011676)

SERC sent URE an initial notice of Compliance Audit. URE submitted a Self-Report stating that it was in violation of CIP-005-1 R3. SERC determined URE failed to implement electronic or manual processes for monitoring and logging at all access points to the ESP 24 hours a day, seven days a week.

Specifically, URE discovered access points, consisting of a firewall and front-end processors, which were not monitoring and logging. According to URE, when the devices were installed they were not properly configured to forward system and access logs to a centralized server that monitors system events related to cybersecurity. SERC verified that URE had a documented logging and monitoring process in place during the time of the violation.

SERC determined the duration of the violation to be from when URE installed the devices, through when URE configured the devices for monitoring and logging.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to monitor and log access to the access points could have resulted in unauthorized attempts to access the ESP without alerting URE. URE partially mitigated the risk because it configured its firewalls on the ESP to deny access by default, and all of the devices were located within an identified PSP with restricted access.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. configured the devices to send logs to the centralized server;
2. verified that the logs were being received; and
3. created a commissioning checklist to include configuration of monitoring methods.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-3c R1 (SERC2013011702)

SERC sent URE an initial notice of Compliance Audit. URE submitted a Self-Report stating that it was in violation of CIP-006 R1. SERC determined URE failed to document the entry and exit of visitors from the PSP. During an approximately five-month period, URE employees escorted several visitors into the PSP without the escorts signing in the visitors using the required form. The employees escorted all the visitors while inside the PSP.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a Self-Report stating that it had also failed to create a completely enclosed six-wall border for all Cyber Assets within the ESP. URE discovered that one PSP had a clear opening of seven feet to the roof deck on top of several walls.

SERC determined the duration of the violation to be from when URE commissioned the PSP, through when URE completed the six-wall border.

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. For the first instance, the escorts were authorized personnel with cybersecurity training and valid PRAs and escorted the visitors at all times while inside the PSP. For the second instance, to gain physical access to the PSP using the breach, an intruder would have to pass a guard, a mantrap, card readers, a biometric reader, and then climb to the breach. Finally, URE houses its CCAs within a six-wall cabinet with card access and a key lock.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. trained applicable personnel on the PSP procedures;
2. emailed all personnel regarding the importance of maintaining complete visitors logs at all PSP locations; and
3. installed a barrier in order to create a complete six-wall border.

URE certified that the above Mitigation Plan requirements were completed.

CIP-006-1 R3 (SERC2013012693)

During a Compliance Audit, SERC determined that URE failed to implement technical controls to monitor for unauthorized access attempts to PSPs. While URE used alarm systems as its monitoring method for physical access, URE's alarms failed to provide immediate notification to personnel responsible for responding to unauthorized access attempts. In addition, URE had not configured one of the PSPs to process door forced open events. URE did have in place a documented process for monitoring physical access during the time of the violation.

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

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to configure PSP access points for door forced open alarms could have allowed unauthorized access to the PSP to remain unnoticed and unchecked, potentially allowing malicious access to CCAs. However, personnel with the required cybersecurity training and PRAs man the first PSP continuously, and URE's PSPs had closed circuit television video monitoring at all access points.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. reconfigured and tested alarms/alerts at the affected PSPs;
2. developed a replacement checklist for quarterly and annual inspection; and
3. updated the applicable procedure and conducted training for the appropriate personnel.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R1 (SERC2013012695)

During a Compliance Audit, SERC determined that URE failed to ensure that new Cyber Assets and significant changes to existing Cyber Assets within the ESP did not adversely affect existing cybersecurity controls. URE was unable to provide the required test results for significant changes to new and to existing Cyber Assets within the ESP. URE had a documented process that required testing of all security-related changes to ensure that the change did not negatively affect or degrade existing cyber security controls. URE provided evidence that it performed some testing on some significant

changes; however, it was unable to provide evidence that all significant changes to new and existing Cyber Assets were adequately tested.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. URE had conducted some testing on its Cyber Assets even though it failed to document the results for each test. Its process for testing significant changes to CCAs was to test the change on a quality assurance system before implementing the change on the production environment. Additionally, an ESP and PSP protected all CCAs, and all individuals with access to the CCAs had valid PRAs.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. developed a training PowerPoint, which emphasized the correct methods to identify significant changes;
2. provided the PowerPoint to the applicable personnel; and
3. created a form for documenting testing results.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R2: R2.1 (SERC2013012694)

During a Compliance Audit, SERC determined that URE failed to enable only those services required for normal and emergency operations. Specifically, one non-critical Cyber Asset, a server, had services enabled that were not required for normal and emergency operations. The services were part of the default installation for this particular device. URE had removed the services on other similar devices.

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

SERC determined that this violation posed a minimal and not serious or substantial risk to the reliability of the BPS. The device was a non-critical Cyber Asset that resided in an ESP, had no connectivity to outside networks, and could not control the BPS.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. reviewed and disabled the ports and services not required for normal and emergency operations;
2. developed differential scripts to track the before and the after regarding the removal of services and ports;
3. documented the changed services;
4. updated baseline documents for each device;
5. updated the change control procedure to require that scripts be run before and after major changes in order to detect unexpected alterations of ports and services; and
6. provided training to the applicable personnel on the updated change control procedure.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R3 (SERC2012009565)

URE submitted a Self-Report to SERC stating that it had failed to implement a patch management program for tracking, evaluating, testing, and installing applicable cybersecurity software patches for all Cyber Assets within the ESP. Specifically, 66% of its Cyber Assets were not included in its documented security patch management program. URE failed to apply patches and service packs to the Cyber Assets at issue.

While SERC was performing its assessment and determining the scope of the violation, it determined during a Compliance Audit that URE had also failed to assess some security patches within 30 calendar days of availability from the mandatory and enforceable date of this Standard until several years later. URE did not have a documented process for patch assessment for several years; however, URE did install some security patches during this period.

SERC determined the duration of the violation to be from the date the Standard became mandatory and enforceable on URE, through when URE updated the process to include all Cyber Assets, and assessed and installed all patches.

SERC determined that this violation posed a serious or substantial risk. Specifically, failing to assess and install security patches potentially exposed URE's CCAs to a number of vulnerabilities, which could

have allowed for a cyber-attack. URE did have some elements in place to protect these Cyber Assets. The Cyber Assets resided within a designated ESP and PSP, both of which required authorization for all individuals to access, and the Cyber Assets had antivirus software installed and monitored.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. assigned identifiers to each device to assist with tracking;
2. assessed all applicable patches;
3. assigned an additional employee to assist with patch implementation;
4. reviewed and updated the templates to supply patch assessment data; and
5. trained the applicable personnel on the updated template.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R4 (SERC2012009647)

URE submitted a Self-Report to SERC stating that it had failed to use antivirus software and other malware prevention tools, where technically feasible, to detect, prevent, deter, and mitigate the introduction, exposure, and propagation of malware on all Cyber Assets within the ESP. Specifically, it failed to install antivirus software or other malicious software tools on switches, routers, remote terminal units, and a digital video recorder. According to URE, these devices were not capable of running an antivirus or prevention tool; however, URE had not submitted a TFE.

While SERC was performing its assessment and determining the scope of the violation, URE submitted a Self-Report stating that it had also failed to install antivirus software on certain CCAs. According to URE, it had installed a monitoring tool incorrectly believing the software was also antivirus and antimalware.

SERC determined the duration of the violation to be from when URE added the devices to production without antivirus software or other malware prevention tools, through when URE installed antivirus software on its systems.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to use antivirus software or malware prevention tools

could have allowed the introduction of malicious software to Cyber Assets exposing them to security vulnerabilities. URE had some elements in place that partially mitigated the risk. The systems were located inside an ESP and configured to send security and system logs to a central server for monitoring and alerting 24 hours a day, seven days a week. In addition, after installation of an antivirus software and a full scan, it was determined none of the systems contained viruses or malware.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. submitted TFEs for the devices that do not support antivirus; and
2. installed antivirus software on the missed devices.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R5 (SERC2012009566)

URE submitted a Self-Report to SERC stating that it had failed to establish and implement technical and procedural controls that enforce access authentication of and accountability for, all user activity and that minimize the risk of unauthorized system access. As part of its Cyber Vulnerability Assessment, URE discovered enabled user accounts on Cyber Assets within the ESP that it did not need for business purposes. Two were shared accounts, and the remaining accounts were local administrator accounts. These administrator accounts were not remotely accessible, and URE used them for the initial installation of vendor software. While SERC was determining the scope of the violation, URE submitted Self-Reports identifying additional issues.

URE failed to require passwords to meet the complexity requirements on 65% of its passwords. Specifically, the passwords were not technically capable of containing alpha, numeric, and "special" characters. URE had not submitted a TFE.

During a quarterly review, URE discovered that it failed to identify the individuals with access to the shared accounts. The accounts applied to network devices identified as CCAs.

URE failed to change default passwords on two Cyber Assets. URE had not checked to verify that it had changed the default accounts or passwords after vendor installation.

Finally, URE failed to change passwords at least annually as required. URE discovered over one hundred expired passwords on workstations. The workstations had a technical password control deployed to force a password change after 365 days; however, the control would only force a password change if there were an attempted login. There was no access to the accounts within the annual period, and the policy and control deployed did not enforce the annual change.

SERC determined the duration of the violation to be from when URE enabled accounts within the ESP that it did not need for business purposes, through when URE completed its Mitigation Plan.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to establish and implement procedural and technical controls for account management increased the risk of unauthorized access to CCAs and weakened the security of the ESP. However, all of the users had the required cybersecurity training as well as valid PRAs and URE protected all CCAs within an ESP and PSP.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. identified the devices with default accounts and removed, disabled, or modified them, as needed;
2. submitted a TFE with compensating measures for those devices that cannot meet password complexity requirements;
3. documented shared accounts for all devices within the ESP;
4. created a commissioning checklist for all devices installed inside an ESP; and
5. created a process to notify users of accounts with passwords that are nearing the 365-day age limit.

URE certified that the above Mitigation Plan requirements were completed.

CIP-007-1 R6 (SERC2012009564)

URE submitted a Self-Report stating that it had failed to implement automated tools or organizational process controls to monitor cybersecurity system events on one or more Cyber Assets inside the ESP. Since their initial deployment, URE did not configure certain servers to send system logs to the centralized server.

While SERC was performing its assessment and determining the scope of the violation, URE submitted Self-Reports stating that it had also failed to review logs of system events related to cybersecurity and maintain records documenting reviewing logs. It failed to review manually event logs for two remote terminal units.

In addition, URE also failed to implement process controls to monitor system events for three Cyber Assets within the ESP. After URE generated log reports, it discovered the absence of logs for the three Cyber Assets. The devices were not technically capable of generating system event logs.

SERC determined the duration of the violation to be from when the Standard became mandatory and enforceable on URE, through when URE configured the servers to forward logs.

SERC determined that this violation posed a moderate risk to the reliability of the BPS, but did not pose a serious or substantial risk. Specifically, failure to log and to monitor cyber system events could have allowed unauthorized access to Cyber Assets to be unnoticed and unchecked. Unauthorized access to its Cyber Assets within the ESPs could have resulted in an undetected security breach. An undetected security breach may have rendered CCAs inoperable, possibly resulting in the loss of monitoring and control of the BPS. However, the devices were all located within a designated ESP and PSP, and individuals with authorized access to the devices had an approved PRA and the required cybersecurity training. In addition, after review of the device logs, URE detected no significant cybersecurity events.

URE's Mitigation Plan to address this violation was submitted as complete to SERC.

URE's Mitigation Plan stated URE had taken the following actions to mitigate the issue and prevent recurrence:

1. identified all of the affected devices and configured them to forward logs to the centralized log server;
2. tested each device to verify that logs were being forwarded;
3. manually reviewed the logs of devices that cannot forward logs to the centralized log server; and
4. updated the TFEs for the devices that are unable to log.

URE certified that the above Mitigation Plan requirements were completed.

Regional Entity's Basis for Penalty

According to the Settlement Agreement, SERC has assessed a penalty of seventy thousand dollars ($70,000) for the referenced violations. In reaching this determination, SERC considered the following factors:

1. URE had prior violation history, which was considered an aggravating factor in the penalty determination;
2. URE had an internal compliance program at the time of the violation which SERC considered a mitigating factor;
3. URE self-reported the violations of CIP-005-1 R1.4, and CIP-007-1 R3, R4, R5, and R6;
4. URE self-reported the violations of CIP-005-1 R3 and CIP-006-3c R1 after receiving notice of an upcoming Compliance Audit;
5. URE was cooperative throughout the compliance enforcement process;
6. there was no evidence of any attempt to conceal a violation nor evidence of intent to do so;
7. the violations of CIP-002-1 R3, CIP-005-1 R1.4, CIP-006-3c R1, and CIP-007-1 R1 and R2.1, posed a minimal risk, and the violations of CIP-005-1 R1, R3, CIP-006-1 R3, and CIP-007-1 R4, R5, and R6 posed a moderate risk, but did not pose a serious or substantial risk to the reliability of the BPS, as discussed above;
8. the violation of CIP-007-1 R3 posed a serious or substantial risk to the reliability of the BPS, as discussed above; and
9. 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 seventy thousand dollars ($70,000) 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 February 10, 2015 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.

In reaching this determination, the NERC BOTCC also considered the factors considered by SERC as listed above.

For the foregoing reasons, the NERC BOTCC approved the Settlement Agreement and believes that the assessed penalty of seventy thousand dollars ($70,000) 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:

Gerald W. Cauley President and Chief Executive Officer North American Electric Reliability Corporation 3353 Peachtree Road NE Suite 600, North Tower Atlanta, GA 30326 (404) 446-2560 Charles A. Berardesco* Senior Vice President and General Counsel North American Electric Reliability Corporation 1325 G Street N.W., Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile charles.berardesco@nerc.net	Sonia C. Mendonça* Deputy General Counsel, Vice President of Compliance and Enforcement North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile sonia.mendonca@nerc.net Edwin G. Kichline* Senior Counsel and Associate Director, Enforcement Processing North American Electric Reliability Corporation 1325 G Street N.W. Suite 600 Washington, DC 20005 (202) 400-3000 (202) 644-8099 – facsimile edwin.kichline@nerc.net

Marisa A. Sifontes* General Counsel Drew R. Slabaugh* Legal Counsel Rebecca A. Lindensmith* Legal Counsel SERC Reliability Corporation 3701 Arco Corporate Drive, Suite 300 Charlotte, NC 28273 (704) 494-7775 (704) 414-5244 (704) 414-5230 (704) 357-7914 – facsimile msifontes@serc1.org dslabaugh@serc1.org rlindensmith@serc1.org	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 *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.

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

Gerald W. Cauley
President and Chief Executive Officer
North American Electric Reliability Corporation
3353 Peachtree Road NE
Suite 600, North Tower
Atlanta, GA 30326
(404) 446-2560

Charles A. Berardesco
Senior Vice President and General Counsel
North American Electric Reliability Corporation
1325 G Street N.W., Suite 600
Washington, DC 20005
(202) 400-3000
(202) 644-8099 – facsimile
charles.berardesco@nerc.net

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

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

cc: Unidentified Registered Entity
SERC Reliability Corporation

Attachments